

#2

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Shinsuke MORIAI**

Serial No.: **Not Yet Assigned**

Filed: **August 20, 2001**

For: **DATA TERMINAL DEVICE CAPABLE OF CONTINUING TO DOWNLOAD
ENCRYPTED CONTENT DATA AND A LICENSE OR REPRODUCE ENCRYPTED
CONTENT DATA WITH ITS CASING IN THE FORM OF A SHELL CLOSED**



CLAIM FOR PRIORITY UNDER 35 U.S.C. 119

Commissioner for Patents
Washington, D.C. 20231

August 20, 2001

Sir:

The benefit of the filing date of the following prior foreign application is hereby requested for the above-identified application, and the priority provided in 35 U.S.C. 119 is hereby claimed:

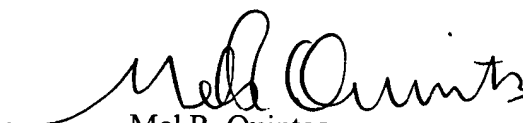
Japanese Appln. No. 2000-286582, filed on September 21, 2000

In support of this claim, the requisite certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the applicant has complied with the requirements of 35 U.S.C. 119 and that the Patent and Trademark Office kindly acknowledge receipt of said certified copy.

In the event that any fees are due in connection with this paper, please charge our Deposit Account No. 01-2340.

Respectfully submitted,
ARMSTRONG, WESTERMAN, HATTORI
McLELAND & NAUGHTON, LLP


Mel R. Quintos
Reg. No. 31,898

Atty. Docket No.: 011049
Suite 1000, 1725 K Street, N.W.
Washington, D.C. 20006
Tel: (202) 659-2930
Fax: (202) 887-0357
MRQ/yap

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2000年 9月21日
September 21, 2000

出 願 番 号
Application Number:

特願2000-286582
Pat. Appln. No. 2000-286582

出 願 人
Applicant(s):

三洋電機株式会社
Sanyo Electric Co., Ltd.



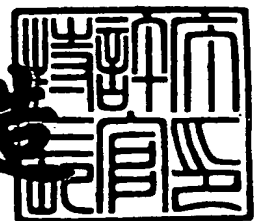
CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月 3日
August 3, 2001

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造

Kozo Oikawa



出証番号 出証特2001-3069771

Shutsu-sho-No. Shutsu-sho-toku 2001-3069771

【書類名】 特許願

【整理番号】 NEC1002161

【提出日】 平成12年 9月21日

【あて先】 特許庁長官殿

【国際特許分類】 G11B 20/10

【発明者】

 【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会
社内

 【氏名】 盛合 真介

【特許出願人】

 【識別番号】 000001889

 【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号

 【氏名又は名称】 三洋電機株式会社

【代理人】

 【識別番号】 100064746

 【弁理士】

 【氏名又は名称】 深見 久郎

【選任した代理人】

 【識別番号】 100085132

 【弁理士】

 【氏名又は名称】 森田 俊雄

【選任した代理人】

 【識別番号】 100091409

 【弁理士】

 【氏名又は名称】 伊藤 英彦

【選任した代理人】

 【識別番号】 100096781

 【弁理士】

 【氏名又は名称】 堀井 豊

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 シェル型データ端末装置

【特許請求の範囲】

【請求項 1】 コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを復号するライセンスキーとが格納された配信サーバから、前記暗号化コンテンツデータおよび前記ライセンスキーをダウンロードし、前記暗号化コンテンツデータを再生するシェル型筐体に包まれたシェル型データ端末装置であって、

外部との通信を行なう通信部と、

前記暗号化コンテンツデータおよび前記ライセンスキーを記録し、認証データの入力を受けて前記認証データを認証した場合にのみ前記記録したライセンスキーを出力するデータ記録装置と、

データ授受を制御するインタフェースと、

制御部と、

前記シェル型筐体の開閉状態を検出する検出部と、

各部に電源を供給制御する電源制御部とを備え、

前記電源制御部は、

前記暗号化コンテンツデータのダウンロードを開始した後に前記検出部により前記シェル型筐体が閉じられたことが検出されると、前記ダウンロードが完了するまで通話に必要な電源を供給するように制御する、シェル型データ端末装置。

【請求項 2】 前記電源制御部は、

前記シェル型筐体が閉じられた後前記ダウンロードが完了すると、前記電源供給を停止したり、データ端末内の前記各部のスタンバイモード機能などを制御して、低消費電力モードに移行させる、請求項 1 に記載のシェル型データ端末装置。

【請求項 3】 コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを復号するライセンスキーとが格納された配信サーバから、前記暗号化コンテンツデータおよび前記ライセンスキーをダウンロードし、前記暗号化コンテンツデータを再生するシェル型筐体に包まれたシェル型デ

ータ端末装置であって、

外部との通信を行なう通信部と、

前記暗号化コンテンツデータおよび前記ライセンスキーを記録し、認証データの入力を受けて前記認証データを認証した場合にのみ前記記録したライセンスキーを出力するデータ記録装置と、

前記データ記録装置に記録される前記暗号化コンテンツデータを再生する再生部と、

データ授受を制御するインタフェースと、

制御部と、

前記シェル型筐体の開閉状態を検出する検出部と、

各部に電源を供給制御する電源制御部とを備え、

前記電源制御部は、

前記暗号化コンテンツデータの再生を開始した後に前記検出部により前記シェル型筐体が閉じられたことが検出されると、前記再生が完了するまで再生処理に必要な電源を供給するように制御する、シェル型データ端末装置。

【請求項 4】 前記電源制御部は、

前記シェル型筐体が閉じられた後、前記再生が完了すると、前記電源供給を停止したり、データ端末内の前記各部のスタンバイモード機能などを制御して、低消費電力モードに移行させる、請求項 3 に記載のシェル型データ端末装置。

【請求項 5】 コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを復号するライセンスキーとが格納された配信サーバから、前記暗号化コンテンツデータおよび前記ライセンスキーをダウンロードしてデータ記録装置に記録し、前記データ記録装置を用いて前記暗号化コンテンツデータを再生するシェル型筐体に包まれたシェル型データ端末装置であって、

外部との通信を行なう通信部と、

データ授受を制御するインタフェースと、

制御部と、

前記シェル型筐体の開閉状態を検出する検出部と、

各部に電源を供給制御する電源制御部とを備え、

前記電源制御部は、

前記暗号化コンテンツデータのダウンロードを開始した後に前記検出部により前記シェル型筐体が閉じられたことが検出されると、前記ダウンロードが完了するまで通話に必要な電源を供給するように制御する、シェル型データ端末装置。

【請求項 6】 前記電源制御部は、

前記シェル型筐体が閉じられた後、前記ダウンロードが完了すると、前記電源供給を停止したり、データ端末内の前記各部のスタンバイモード機能などを制御して、低消費電力モードに移行させる、請求項 5 に記載のシェル型データ端末装置。

【請求項 7】 コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを復号するライセンスキーとが格納された配信サーバから、前記暗号化コンテンツデータおよび前記ライセンスキーをダウンロードしてデータ記録装置に記録し、前記データ記録装置を用いて前記暗号化コンテンツデータを再生するシェル型筐体に包まれたシェル型データ端末装置であって、外部との通信を行なう通信部と、

データ授受を制御するインタフェースと、

制御部と、

前記データ記録装置に記録される前記暗号化コンテンツデータを再生する再生部と、

前記シェル型筐体の開閉状態を検出する検出部と、

各部に電源を供給制御する電源制御部とを備え、

前記電源制御部は、

前記暗号化コンテンツデータの再生を開始した後に前記検出部により前記シェル型筐体が閉じられたことが検出されると、前記再生が完了するまで再生処理に必要な電源を供給するように制御する、シェル型データ端末装置。

【請求項 8】 前記電源制御部は、

前記シェル型筐体が閉じられた後、前記再生が完了すると、前記電源供給を停止したり、データ端末内の前記各部のスタンバイモード機能などを制御して、低消費電力モードに移行させる、請求項 7 に記載のシェル型データ端末装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【0 0 0 2】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0 0 0 3】

このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0 0 0 4】

したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0 0 0 5】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0 0 0 6】

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディス

ク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】

しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】

このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】

【発明が解決しようとする課題】

ところで、従来のシェル型携帯電話機は、シェル型の筐体が閉じられると通話が切断され、低消費電力モードになる。

【0010】

より具体的には、図19を参照して、電源がオフされている状態にあるとする（ステップS1）。電源キーが押されたか否かを検出する（ステップS2）。電源キーが押された場合には、液晶表示、バックライト等が点灯する（ステップS3）。電源キーが押されていないければ、ステップS1に戻る。

【0011】

そして、待ち受け状態になり（ステップS4）、通話キーが押されたかを判定する（ステップS5）。通話キーが押されると、通話状態になる（ステップS6）。通話キーが押されていないければ、シェル型筐体の開閉状態を判定するステップS10に移る。

【0012】

通話中には、通話を切断する切断キーが押されたかを判定する（ステップS7

）。切断キーが押されたら、ステップ S 4 に戻る。

【0013】

切断キーが押されていないければ、シェル型筐体が閉じられたか否かを判定する（ステップ S 8）。閉じられていないければ、ステップ S 6 に戻る。

【0014】

閉じられた場合には、通話が切断され（ステップ S 9）、シェル型筐体が閉じられた状態での待ち受け状態になる（ステップ S 11）。ステップ S 11 の状態では、低消費電源モードにある。

【0015】

ステップ S 10 においてシェル型筐体が閉じられた状態であると判定されるとステップ S 11 に移り、開いた状態にあると判定されるとステップ S 4 に移る。

【0016】

ステップ S 11 の状態で、シェル型筐体の開閉が判定され（ステップ S 12）、閉じた状態であるとステップ S 11 を維持し、開いた状態になるとステップ S 3 に移る。

【0017】

すなわち、従来のシェル型携帯電話機であれば、通話（メール、パソコン通信等含む）中には必ずシェル型筐体を開いた状態にしなければならなかった。

【0018】

従来のシェル型携帯電話機では、著作権を十分に保護した暗号化コンテンツデータやライセンスキーをダウンロードし再生することができない。また、たとえ暗号化コンテンツデータやライセンスキーをダウンロードし再生可能なように構成したとしても、ダウンロード中または再生中はシェル型筐体を開けた状態で放置しなければならない。特に音楽コンテンツのような大量のデータをダウンロードし再生する際には、長時間、シェル型筐体を開けた状態にしておかなくてはならないのは不便である。

【0019】

そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、シェル型筐体が閉められても、継続して暗号化コンテンツデータやライセ

ンスキーをダウンロードし、または再生することができるデータ端末装置を提供することである。

【0020】

【課題を解決するための手段および発明の効果】

この発明のある局面によるシェル型データ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを復号するライセンスキーとが格納された配信サーバから、暗号化コンテンツデータおよびライセンスキーをダウンロードし、暗号化コンテンツデータを再生するシェル型筐体に包まれたシェル型データ端末装置であって、外部との通信を行なう通信部と、暗号化コンテンツデータおよびコンテンツキーを記録し、認証データの入力を受けて前記認証データを認証した場合にのみ前記記録したライセンスキーを出力するデータ記録装置と、インタフェースと、制御部と、シェル型筐体の開閉状態を検出する検出部と、各部に電源を供給制御する電源制御部とを備える。

【0021】

電源制御部は、暗号化コンテンツデータのダウンロードを開始した後に検出部により前記シェル型筐体が閉じられたことが検出されると、ダウンロードが完了するまでは通話に必要な電源を供給するように制御する。好ましくは、電源制御部は、シェル型筐体が閉じられた後ダウンロードが完了すると、電源供給を停止したり、データ端末内の前記各部のスタンバイモード機能などを制御して、低消費電力モードに移行させる。

【0022】

または、シェル型データ端末装置は、再生部を備え、電源制御部は、暗号化コンテンツデータの再生を開始した後に検出部によりシェル型筐体が閉じられたことが検出されると、再生が完了するまで再生処理に必要な電源を供給するように制御する。好ましくは、電源制御部は、シェル型筐体が閉じられた後再生が完了すると、電源供給を停止したり、データ端末内の各部のスタンバイモード機能などを制御して、低消費電力モードに移行させる。

【0023】

この発明のさらなる局面によるシェル型データ端末装置は、コンテンツデータ

を暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを復号するライセンスキーとが格納された配信サーバから、暗号化コンテンツデータおよびライセンスキーをダウンロードしてデータ記録装置に記録し、データ記録装置を用いて暗号化コンテンツデータを再生するシェル型筐体に包まれたシェル型データ端末装置であって、通信部と、インタフェースと、制御部と、検出部と、電源制御部とを備える。

【 0 0 2 4 】

電源制御部は、暗号化コンテンツデータのダウンロードを開始した後に検出部によりシェル型筐体が閉じられたことが検出されると、ダウンロードが完了するまで通話に必要な電源を供給するように制御する。好ましくは、電源制御部は、シェル型筐体が閉じられた後ダウンロードが完了すると、電源供給を停止したり、データ端末内の各部のスタンバイモード機能などを制御して、低消費電力モードに移行させる。

【 0 0 2 5 】

または、シェル型データ端末装置は再生部を備え、電源制御部は、暗号化コンテンツデータの再生を開始した後に検出部によりシェル型筐体が閉じられたことが検出されると、再生が完了するまでは再生処理に必要な電源を供給するように制御する。好ましくは、電源制御部は、シェル型筐体が閉じられた後再生が完了すると、電源供給を停止したり、データ端末内の各部のスタンバイモード機能などを制御して、低消費電力モードに移行させる。

【 0 0 2 6 】

従って、上記シェル型データ端末装置によると、暗号化コンテンツデータのダウンロード中にシェル型筐体を閉じて、ダウンロードを完了させることができる。特に、音楽コンテンツ等の大量のデータをダウンロードする場合、シェル型筐体を開けた状態で放置する必要がなくなる。

【 0 0 2 7 】

また、上記シェル型データ端末装置によると、暗号化コンテンツデータの再生中にシェル型筐体を閉じて、再生を完了させることができる。したがって、シェル型筐体を開けた状態で放置する必要がなくなる。

【 0 0 2 8 】

さらに、上記シェル型データ端末装置によると、暗号化コンテンツデータを著作権を十分に保護しながらダウンロードし、再生することができる。

【 0 0 2 9 】

【発明の実施の形態】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【 0 0 3 0 】

〔実施の形態 1〕

図 1 は、本発明によるデータ端末装置が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【 0 0 3 1 】

なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画画像データ等を配信する場合においても適用することが可能なものである。また、他の情報通信網を介して配信する場合においても適用可能である。

【 0 0 3 2 】

図 1 を参照して、著作権の存在する音楽データを管理するライセンスサーバ 1 0 は、データ配信を求めてアクセスして来た携帯電話ユーザ 1 の携帯電話機 1 0 0 に装着されたメモリカード 1 1 0 が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア 2 0 である携帯電話会社に、このような暗号化コンテンツデータを与える。

【 0 0 3 3 】

配信キャリア 2 0 は、自己の携帯電話網を通じて、各携帯電話ユーザからの配

信要求（配信リクエスト）をライセンスサーバ 1 0 に中継する。ライセンスサーバ 1 0 は、配信リクエストがあると、メモリカード等が正規の機器であることを確認し、要求されたコンテンツデータをさらに暗号化した上で配信キャリア 2 0 の携帯電話網を介して、各携帯電話ユーザの携帯電話機を介して装着されたメモリカードに対してコンテンツデータを配信する。

【 0 0 3 4 】

図 1 においては、たとえば携帯電話ユーザ 1 の携帯電話機 1 0 0 には、着脱可能なメモリカード 1 1 0 が装着される構成となっている。メモリカード 1 1 0 は、携帯電話機 1 0 0 により受信された暗号化コンテンツデータを受取り、格納する。また、上記配信にあたって行なわれた認証処理によりライセンスキーを受取り、データを格納する。そして、暗号化データを復号した上で、携帯電話機 1 0 0 中の音楽再生部（図示せず）に与える。

【 0 0 3 5 】

さらに、たとえば携帯電話ユーザは、携帯電話機 1 0 0 に接続したヘッドホン 1 3 0 等を介してライセンスキーにより暗号化コンテンツデータを復号して「再生」し、聴取することが可能である。

【 0 0 3 6 】

以下では、このようなライセンスサーバ 1 0 と配信キャリア 2 0 と併せて、配信サーバ 3 0 と総称することにする。

【 0 0 3 7 】

また、このような配信サーバ 3 0 から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【 0 0 3 8 】

携帯電話機 1 0 0 は、図 2（a）～2（c）に示すようにシェル型筐体を有する。シェル型筐体は、本体部分 3 0 0 0、蓋部分 3 0 0 2 および可動接合部 3 0 0 4 で構成される。たとえば、本体部分 3 0 0 0 には、ユーザがデータを入力するキー 1 1 0 8 が配置され、蓋部分 3 0 0 2 には、データを表示するディスプレイ 1 1 1 0 が配置されている。可動接合部 3 0 0 4 により、携帯電話機 1 0 0 は、（a）-（b）開いた状態から（c）閉じた状態に、（c）閉じた状態から（

a) - (b) 開いた状態になる。

【0039】

後述するように、携帯電話機100に含まれるシェル開閉検出部1117は、シェル型筐体の開閉状態を検出する。一例としては、本体部分3000の表面にある特定部3008aと蓋部分3002の表面にある特定部3008bとが接触するとシェル型筐体が閉じた状態になったと判断する。

【0040】

このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0041】

しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0042】

このような構成において、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号化鍵を配信するための方式である。第2には、配信したいコンテンツデータを暗号化する方式そのものである。第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。そして、第4には、シェル型筐体を閉じて、継続中の処理モード（たとえば、ダウンロード処理、再生処理）を完了させることができる構成である。

【0043】

第1の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生

装置（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成、ならびに携帯電話機において、シェル型筐体が開じられても、継続中のダウンロード処理、再生処理を完了させる構成を示す。

【 0 0 4 4 】

図 3 は、図 1 に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【 0 0 4 5 】

まず、配信サーバ 3 0 より配信されるデータについて説明する。Data は、音楽データ等のコンテンツデータである。コンテンツデータ Data には、ライセンスキー Kc で復号可能な暗号化が施される。ライセンスキー（「コンテンツキー」とも言う。以下同じ。）Kc によって復号可能な暗号化が施された暗号化コンテンツデータ {Data} Kc がこの形式で配信サーバ 3 0 より携帯電話ユーザに配布される。

【 0 0 4 6 】

なお、以下においては、{Y} X という表記は、データ Y を、復号鍵 X により復号可能な暗号化を施したことを示すものとする。

【 0 0 4 7 】

さらに、配信サーバ 3 0 からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報 Data-inf が配布される。また、ライセンス情報としては、コンテンツデータ Data を識別するためのコードであるコンテンツ ID およびライセンスの発行を特定できる管理コードであるライセンス ID や、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件 AC に基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報 AC 1 および再生回路における制御情報である再生回路制御情報 AC 2 等が存在する。以後、ライセンスキー Kc とコンテンツ ID とライセンス ID とアクセス制御情報 AC 1 と再生回路制御情報 AC 2 とを併せて、ライセンスと総称することとする。

【 0 0 4 8 】

図 4 は、図 1 に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【 0 0 4 9 】

第 1 の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生するデータ端末装置（携帯電話機）のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリスト C R L （ C l a s s R e v o c a t i o n L i s t ） の運用を行なう。以下では、必要に応じて記号 C R L によって禁止クラスリスト内のデータを表わすこともある。

【 0 0 5 0 】

禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止されるデータ端末装置およびメモリカードのクラスをリストアップした禁止クラスリストデータ C R L が含まれる。

【 0 0 5 1 】

禁止クラスリストデータ C R L は、配信サーバ 3 0 内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データ C R L _ d a t を配信サーバ 3 0 側より発生して、これに応じてメモリカード内の禁止クラスリスト C R L が書替えられる構成とする。また、禁止クラスリストのバージョンについては、C R L _ v e r をメモリカード側より出力し、これを配信サーバ 3 0 側で確認することによってバージョン管理を実行する。差分データ C R L _ d a t には新たなバージョンの情報も含まれる。また、バージョン情報として、更新日時を用いることも可能である。

【 0 0 5 2 】

このように、禁止クラスリスト C R L を、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、データ端末装置およびメモリカードの種類に固有の復号鍵が破られた、データ端末装置およびメモリカードへのライセンスキーの供給を禁止する。このため、データ端末装置で

はコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【 0 0 5 3 】

このように、メモリカード内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストCRLの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタンスモジュール (Tamper Resistance Module) に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【 0 0 5 4 】

データ端末装置およびメモリカードには固有の公開暗号鍵K P p nおよびK P m c i がそれぞれ設けられ、公開暗号鍵K P p nおよびK P m c i はデータ端末装置に固有の秘密復号鍵K p nおよびメモリカード固有の秘密復号鍵K m c i によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、データ端末装置の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【 0 0 5 5 】

また、再生回路およびメモリカードのクラス証明書として、C r t f nおよびC m c i がそれぞれ設けられる。

【 0 0 5 6 】

これらのクラス証明書は、メモリカードおよびコンテンツ再生部（携帯電話機）のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【 0 0 5 7 】

これらのメモリカードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、認証データ {K P m c i / / C m c i} K P m a および {K P p n / / C r t f n} K P m a の形式で、出荷時にメモリカードおよび携帯電話機にそ

れぞれ記録される。後ほど詳細に説明するが、K P m a は配信システム全体で共通の公開認証鍵である。

【 0 0 5 8 】

図 5 は、図 1 に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【 0 0 5 9 】

メモ리카ード外とメモ리카ード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ 3 0、携帯電話機 1 0 0、メモ리카ード 1 1 0 において生成される共通鍵 K s 1 ~ K s 3 が用いられる。

【 0 0 6 0 】

ここで、共通鍵 K s 1 ~ K s 3 は、配信サーバ、携帯電話機もしくはメモ리카ード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 K s 1 ~ K s 3 を「セッションキー」とも呼ぶこととする（なお、鍵は、キーと記す場合もある）。

【 0 0 6 1 】

これらのセッションキー K s 1 ~ K s 3 は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモ리카ードによって管理される。具体的には、セッションキー K s 1 は、配信サーバによって配信セッションごとに発生される。セッションキー K s 2 は、メモ리카ードによって配信セッションおよび再生セッションごとに発生し、セッションキー K s 3 は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【 0 0 6 2 】

また、メモ리카ード 1 1 0 内のデータ処理を管理するための鍵として、メモ리카ードという媒体ごとに設定される公開暗号鍵 K P m と、公開暗号鍵 K P m で暗

号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵 K_m が存在する。

【 0 0 6 3 】

図 6 は、図 1 に示したライセンスサーバ 1 0 の構成を示す概略ブロック図である。

【 0 0 6 4 】

ライセンスサーバ 1 0 は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンス ID 等の配信情報を保持するための情報データベース 3 0 4 と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース 3 0 2 と、禁止クラスリスト CRL を管理する CRL データベース 3 0 6 と、情報データベース 3 0 4、課金データベース 3 0 2 および CRL データベース 3 0 6 からのデータをデータバス B S 1 を介して受取り、所定の処理を行なうためのデータ処理部 3 1 0 と、通信網を介して、配信キャリア 2 0 とデータ処理部 3 1 0 との間でデータ授受を行なうための通信装置 3 5 0 とを備える。

【 0 0 6 5 】

データ処理部 3 1 0 は、データバス B S 1 上のデータに応じて、データ処理部 3 1 0 の動作を制御するための配信制御部 3 1 5 と、配信制御部 3 1 5 に制御されて、配信セッション時にセッションキー K_s を発生するためのセッションキー発生部 3 1 6 と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ $\{K P m c i / / C m c i\}$ $K P m a$ を通信装置 3 5 0 およびデータバス B S 1 を介して受けて、公開認証鍵 $K P m a$ による復号処理を行なう復号処理部 3 1 2 と、セッションキー発生部 3 1 6 より生成されたセッションキー K_s を復号処理部 3 1 2 によって得られた公開暗号鍵 $K P m c i$ を用いて暗号化して、データバス B S 1 に出力するための暗号化処理部 3 1 8 と、セッションキー K_s によって暗号化された上で送信されたデータをデータバス B S 1 より受けて、復号処理を行なう復号処理部 3 2 0 とを含む。

【 0 0 6 6 】

データ処理部 3 1 0 は、さらに、配信制御部 3 1 5 から与えられるライセンス

キー K c および再生回路制御情報 A C 2 を、復号処理部 3 2 0 によって得られたメモリカード固有の公開暗号鍵 K P m によって暗号化するための暗号化処理部 3 2 6 と、暗号化処理部 3 2 6 の出力を、復号処理部 3 2 0 から与えられるセッションキー K s 2 によってさらに暗号化してデータベース B S 1 に出力するための暗号化処理部 3 2 8 とを含む。

【 0 0 6 7 】

ライセンスサーバ 1 0 の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【 0 0 6 8 】

図 7 は、図 1 に示した携帯電話機 1 0 0 の構成を説明するための概略ブロック図である。

【 0 0 6 9 】

携帯電話機 1 0 0 は、携帯電話網により無線伝送される信号を受信するためのアンテナ 1 1 0 2 と、アンテナ 1 1 0 2 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1 1 0 2 に与えるための送受信部 1 1 0 4 と、携帯電話機 1 0 0 の各部のデータ授受を行なうためのデータベース B S 2 と、データベース B S 2 を介して携帯電話機 1 0 0 の動作を制御するためのコントローラ 1 1 0 6 とを含む。

【 0 0 7 0 】

携帯電話機 1 0 0 は、さらに、外部からの指示を携帯電話機 1 0 0 に与えるためのキー操作部 1 1 0 8 と、コントローラ 1 1 0 6 等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ 1 1 1 0 と、通常の通話動作において、データベース B S 2 を介して与えられる受信データに基づいて音声を再生するための音声再生部 1 1 1 2 とを含む。

【 0 0 7 1 】

携帯電話機 1 0 0 は、さらに、音声再生部 1 1 1 2 の出力をデジタル信号からアナログ信号に変換する D A 変換器 1 1 1 3 と、D A 変換器 1 1 1 3 の出力を外部出力装置等へ出力するための端子 1 1 1 4 とを含む。

【 0 0 7 2 】

携帯電話機100は、さらに、配信サーバ30からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード110と、メモリカード110とデータバスBS2との間のデータの授受を制御するためのメモリインタフェース1200とを含む。

【0073】

携帯電話機100は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵Kp1およびクラス証明書Crtf1を公開復号鍵Kpmaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kp1//Crtf1} Kpmaを保持する認証データ保持部1202を含む。

【0074】

携帯電話機100は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるKp1を保持するKp1保持部1204と、データバスBS2から受けたデータをKp1によって復号しメモリカード110によって発生されたセッションキーKs2を得る復号処理部1206とを含む。

【0075】

携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でデータバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1210と、生成されたセッションキーKs3を復号処理部1206によって得られたセッションキーKs2によって暗号化しデータバスBS2に出力する暗号化処理部1208とを含む。

【0076】

携帯電話機100は、さらに、データバスBS2上のデータをセッションキーKs3によって復号して出力する復号処理部1212とを含む。

【0077】

携帯電話機100は、さらに、データバスBS2より暗号化コンテンツデータ{Data} Kcを受けて、復号処理部1212より取得したライセンスキーKcによって復号しコンテンツデータを出力する復号処理部1214と、復号処理

部 1 2 1 4 の出力を受けてコンテンツデータを再生するための音楽再生部 1 2 1 6 と、音楽再生部 1 2 1 6 の出力をデジタル信号からアナログ信号に変換する D A 変換器 1 2 1 8 と、D A 変換器 1 1 1 3 と D A 変換器 1 2 1 8 との出力を受けて、動作モードに応じて選択的に端子 1 1 1 4 または端子 1 2 2 0 から出力するためのスイッチ 1 2 2 2 と、スイッチ 1 2 2 2 の出力を受けて、ヘッドホン 1 3 0 と接続するための接続端子 1 2 2 4 とを含む。

【 0 0 7 8 】

携帯電話機 1 0 0 はさらに、コントローラ 1 1 0 6 の制御に基づき、携帯電話機 1 0 0 に含まれる各回路に動作電源を供給するか否かの制御を行う電源制御部 1 1 1 6 および携帯電話機 1 0 0 のシェル型筐体が閉じられた状態か開かれた状態かを検出するシェル開閉検出部 1 1 1 7 を含む。シェル開閉検出部 1 1 1 7 における検出結果は、データバス B S 2 を介してコントローラ 1 1 0 6 に転送される。

【 0 0 7 9 】

コントローラ 1 1 0 6 は、後述するようにシェル開閉検出部 1 1 1 7 の検出結果に応じて、電源制御部 1 1 1 6 の電源供給処理、データダウンロード処理、データの再生処理等を制御する。

【 0 0 8 0 】

なお、図 7 においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【 0 0 8 1 】

携帯電話機 1 0 0 の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【 0 0 8 2 】

図 8 は、メモリカード 1 1 0 の構成を説明するための概略ブロック図である。

既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、K P m c i および K m c i が設けられ、メモリカードのクラス証明書 C m c i が設けられるが、メモリカード 1 1 0 においては、これらは自然数 $i = 1$ でそ

れぞれ表わされるものとする。

【0083】

したがって、メモリカード110は、認証データ {K P m c 1 / / C m c 1} K P m a を保持する認証データ保持部1400と、メモリカードの種類ごとに設定される固有の復号鍵であるK m c 1 を保持するK m c 保持部1402と、メモリカードごとに固有に設定される秘密復号鍵K m 1 を保持するK m 1 保持部1421と、K m 1 によって復号可能な公開暗号鍵K P m 1 を保持するK P m 1 保持部1416とを含む。認証データ保持部1400は、メモリカードの種類およびクラスごとにそれぞれ設定される公開暗号鍵K P m c 1 およびクラス証明書C m c 1 を公開認証鍵K P m a で復号することでその正当性を認証できる状態に暗号化した認証データ {K P m c 1 / / C m c 1} K P m a として保持する。

【0084】

このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモリカード単位で実行することが可能になる。

【0085】

メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1201を介して授受するデータバスB S 3 と、データバスB S 3 にメモリインタフェース1200から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵K m c 1 をK m c 1 保持部1402から受けて、配信サーバ30が配信セッションにおいて生成したセッションキーK s 1 を接点P a に出力する復号処理部1404と、K P m a 保持部1414から認証鍵K P m a を受けて、データバスB S 3 に与えられるデータからK P m a による復号処理を実行して復号結果を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1444によって選択的に与えられるデータを暗号化してデータバスB S 3 に出力する暗号化処理部1406とを含む。

【0086】

メモリカード110は、さらに、配信、および再生の各セッションにおいてセ

セッションキー $Ks2$ を発生するセッションキー発生部 1418 と、セッションキー発生部 1418 の出力したセッションキー $Ks2$ を復号処理部 1408 によって得られる公開暗号鍵 $KPpn$ もしくは $KPmci$ によって暗号化してデータバス $BS3$ に送出する暗号化処理部 1410 と、データバス $BS3$ よりセッションキー $Ks2$ によって暗号化されたデータを受けてセッションキー発生部 1418 より得たセッションキー $Ks2$ によって復号し、復号結果をデータバス $BS4$ に送出する復号処理部 1412 とを含む。

【0087】

メモリカード 110 は、さらに、データバス $BS3$ 上のデータを公開暗号鍵 $KPm1$ と対をなすメモリカード 110 固有の秘密復号鍵 $Km1$ によって復号するための復号処理部 1422 と、公開暗号鍵 $KPm1$ で暗号化されている、ライセンスキー Kc 、再生回路制御情報 $AC2$ および再生情報（コンテンツ ID 、ライセンス ID 、アクセス制御情報 $AC1$ ）と、暗号化されていない禁止クラスリストのバージョン更新のための差分データ CRL_dat によって逐次更新される禁止クラスリストデータ CRL とをデータバス $BS4$ より受けて格納するとともに、暗号化コンテンツデータ $\{Data\}$ Kc および付加情報 $Data-inf$ をデータバス $BS3$ より受けて格納するためのメモリ 1415 とを含む。メモリ 1415 は、例えば半導体メモリによって構成される。

【0088】

メモリカード 110 は、さらに、復号処理部 1422 によって得られるライセンス ID 、コンテンツ ID およびアクセス制限情報 $AC1$ を保持するためのライセンス情報保持部 1440 と、データバス $BS3$ を介して外部との間でデータ授受を行ない、データバス $BS4$ との間で再生情報等を受けて、メモリカード 110 の動作を制御するためのコントローラ 1420 とを含む。

【0089】

ライセンス情報保持部 1440 は、データバス $BS4$ との間でライセンス ID 、コンテンツ ID およびアクセス制限情報 $AC1$ のデータの授受が可能である。ライセンス情報保持部 1440 は、 N 個（ N ：自然数）のバンクを有し、各ライセンスに対応するライセンス情報をバンクごとに保持する。

【0090】

なお、図8において、実線で囲んだ領域は、メモリカード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール (T a m p e r R e s i s t a n c e M o d u l e) である。

【0091】

もちろん、メモリ1415も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図8に示したような構成とすることで、メモリ1415中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ1415中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ1415を設ける必要がないので、製造コストが低減されるという利点がある。

【0092】

次に、図1に示すデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

【0093】

図9および図10は、図1に示すデータ配信システムにおけるコンテンツの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第1および第2のフローチャートである。

【0094】

図9および図10においては、携帯電話ユーザ1が、メモリカード110を用いることで、携帯電話機100を介して配信サーバ30から音楽データであるコンテンツデータの配信を受ける場合の動作を説明している。

【0095】

まず、携帯電話ユーザ1の携帯電話機100から、携帯電話ユーザ1によるキー操作部1108のキーボタンの操作等によって、配信リクエストがなされる（

ステップ S 1 0 0)。

【 0 0 9 6 】

メモ리카ード 1 1 0 においては、この配信リクエストに応じて、認証データ保持部 1 4 0 0 より認証データ { K P m c 1 / / C m c 1 } K P m a が出力される (ステップ S 1 0 2)。

【 0 0 9 7 】

携帯電話機 1 0 0 は、メモ리카ード 1 1 0 からの認証のための認証データ { K P m c 1 / / C m c 1 } K P m a に加えて、コンテンツ ID、ライセンス購入条件のデータ AC とを配信サーバ 3 0 に対して送信する (ステップ S 1 0 4)。

【 0 0 9 8 】

配信サーバ 3 0 では、携帯電話機 1 0 0 からコンテンツ ID、認証データ { K P m c 1 / / C m c 1 } K P m a、ライセンス購入条件データ AC を受信し (ステップ S 1 0 6)、復号処理部 3 1 2 においてメモ리카ード 1 1 0 から出力された認証データを公開認証鍵 K P m a で復号処理を実行する (ステップ S 1 0 8)。

【 0 0 9 9 】

配信制御部 3 1 5 は、復号処理部 3 1 2 における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモ리카ード 1 1 0 が正規のメモ리카ードからの公開暗号鍵 K P m c 1 と証明書 C m c 1 を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう (ステップ S 1 1 0)。正当な認証データであると判断された場合、配信制御部 3 1 5 は、公開暗号鍵 K P m c 1 および証明書 C m c 1 を承認し、受理する。そして、次の処理 (ステップ S 1 1 2) へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵 K P m c 1 および証明書 C m c 1 を受理しないで処理を終了する (ステップ S 1 7 0)。

【 0 1 0 0 】

認証の結果、正規の機器であることが認識されると、配信制御部 3 1 5 は、次に、メモ리카ード 1 1 0 のクラス証明書 C m c 1 が禁止クラスリスト C R L にリストアップされているかどうかを C R L データベース 3 0 6 に照会し、これらの

クラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップ S 1 7 0）。

【0 1 0 1】

一方、メモリカード 1 1 0 のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップ S 1 1 2）。

【0 1 0 2】

認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ 3 0 において、セッションキー発生部 3 1 6 は、配信のためのセッションキー K s 1 を生成する。セッションキー K s 1 は、復号処理部 3 1 2 によって得られたメモリカード 1 1 0 に対応する公開暗号鍵 K P m c 1 によって、暗号化処理部 3 1 8 によって暗号化される（ステップ S 1 1 4）。

【0 1 0 3】

暗号化されたセッションキー K s 1 は、{ K s 1 } K m c 1 として、データバス B S 1 および通信装置 3 5 0 を介して外部に出力される（ステップ S 1 1 6）。

【0 1 0 4】

携帯電話機 1 0 0 が、暗号化されたセッションキー { K s 1 } K m c 1 を受信すると（ステップ S 1 1 8）、メモリカード 1 1 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス B S 3 に与えられた受信データを、復号処理部 1 4 0 4 が、保持部 1 4 0 2 に保持されるメモリカード 1 1 0 固有の秘密復号鍵 K m c 1 により復号処理することにより、セッションキー K s 1 を復号し抽出する（ステップ S 1 2 0）。

【0 1 0 5】

コントローラ 1 4 2 0 は、配信サーバ 3 0 で生成されたセッションキー K s 1 の受理を確認すると、セッションキー発生部 1 4 1 8 に対して、メモリカード 1 1 0 において配信動作時に生成されるセッションキー K s 2 の生成を指示する。

【0 1 0 6】

また、配信セッションにおいては、コントローラ 1 4 2 0 は、メモリカード 1

10内のメモリ1415に記録されている禁止クラスリストの状態（バージョン）に関連する情報として、リストのバージョンデータCRL__verをメモリ1415から抽出してデータバスBS4に出力する。

【0107】

暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1404より与えられるセッションキーKs1によって、切換スイッチ1444および1446の接点を順次切換えることによって与えられるセッションキーKs2、公開暗号鍵Kpm1および禁止クラスリストのバージョンデータCRL__verを1つのデータ列として暗号化して、{Ks2//Kpm1//CRL__ver} Ks1をデータバスBS3に出力する（ステップS122）。

【0108】

データバスBS3に出力された暗号化データ {Ks2//Kpm1//CRL__ver} Ks1は、データバスBS3から端子1201およびメモリインタフェース1200を介して携帯電話機100に出力され、携帯電話機100から配信サーバ30に送信される（ステップS124）。

【0109】

配信サーバ30は、暗号化データ {Ks2//Kpm1//CRL__ver} Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモリカード110で生成されたセッションキーKs2、メモリカード110固有の公開暗号鍵Kpm1およびメモリカード110における禁止クラスリストのバージョンデータCRL__verを受理する（ステップS126）。

【0110】

禁止クラスリストのバージョン情報CRL__verは、データバスBS1を介して配信制御部315に送られ、配信制御部315は、受理したバージョンデータCRL__verに従って、当該CRL__verのバージョンとCRLデータベース306内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データCRL__datを生成する（ステップS128）。

【0111】

さらに、配信制御部315は、ステップS106で取得したコンテンツIDおよびライセンス購入条件データACに従って、ライセンスID、アクセス制限情報AC1および再生回路制御情報AC2を生成する（ステップS130）。さらに、暗号化コンテンツデータを復号するためのライセンスキーKcを情報データベース304より取得する（ステップS132）。

【0112】

図10を参照して、配信制御部315は、生成したライセンス、すなわち、ライセンスキーKc、再生回路制御情報AC2、ライセンスID、コンテンツID、およびアクセス制限情報AC1を暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモリカード110固有の公開暗号鍵Kpm1によってライセンスを暗号化する（ステップS136）。暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がデータバスBS1を介して供給する禁止クラスリストの差分データCRL_datとを受けて、メモリカード110において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データは、データバスBS1および通信装置350を介して携帯電話機100に送信される（ステップS138）。

【0113】

このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0114】

携帯電話機100は、送信された暗号化データ（{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1//CRL_dat} Ks2を受信し（ステップS140）、メモリインタフェース1200を介してメモリカード110へ出力する。メモリカード110においては、メモリインタフェース1200を介して、データバスBS3に与えられた受信データを復号処理部14

12によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてデータバスBS3の受信データを復号しデータバスBS4に出力する（ステップS142）。

【0115】

この段階で、データバスBS4には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1と、CRL_datとが出力される。コントローラ1420の指示によって、暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、メモリ1415に記録される（ステップS144）。一方、暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、復号処理部1422において、秘密復号鍵Km1によって復号され、ライセンスのうち、メモリカード110内で参照されるライセンスID、コンテンツIDおよびアクセス制限情報AC1のみが受理される（ステップS146）。

【0116】

コントローラ1420は、受理したCRL_datに基づいて、メモリ1415内の禁止クラスリストデータCRLおよびそのバージョンを更新する（ステップS148）。さらに、ライセンスID、コンテンツIDおよびアクセス制限情報AC1については、ライセンス情報保持部1440に記録される（ステップS150）。

【0117】

ステップS150までの処理がメモリ回路で正常に終了した段階で、携帯電話機100から配信サーバ30にコンテンツデータの配信要求がなされる（ステップS152）。

【0118】

配信サーバ30は、コンテンツデータの配信要求を受けて、情報データベース304より、暗号化コンテンツデータ{Data} Kcおよび付加情報Data-infを取得して、これらのデータをデータバスBS1および通信装置350を介して出力する（ステップS154）。

【0119】

携帯電話機100は、{Data}Kc//Data-infを受信して、暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infを受理する(ステップS156)。暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infは、メモリインタフェース1200および端子1201を介してメモリカード110のデータバスBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infがそのままメモリ1415に記録される(ステップS158)。

【0120】

さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され(ステップS160)、配信サーバ30で配信受理を受信すると(ステップS162)、課金データベース302への課金データの格納等を伴って、配信終了の処理が実行され(ステップS164)、全体の処理が終了する(ステップS170)。

【0121】

このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信できた公開暗号鍵Kpp1およびKpmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵Kpp1およびKpmc1による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0122】

次に、図11および図12を参照してメモリカード110に配信されたコンテンツデータの携帯電話機100における再生動作について説明する。図11を参照して、再生動作の開始とともに、携帯電話機100のユーザ1からキー操作部1108を介して再生指示が携帯電話機100にインプットされる(ステップS

200)。そうすると、コントローラ1106は、データバスBS2を介して認証データ保持部1202から認証データ{KPp1//Crtf1}KPmaを読み出し、メモリアンタフェース1200を介してメモリカード110へ認証データ{KPp1//Crtf1}KPmaを入力する(ステップS201)。

【0123】

そうすると、メモリカード110は、認証データ{KPp1//Crtf1}KPmaを受理する(ステップS202)。そして、メモリカード110の復号処理部1408は、受理した認証データ{KPp1//Crtf1}KPmaを、KPma保持部1414に保持された公開認証鍵KPmaによって復号し(ステップS203)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ{KPp1//Crtf1}KPmaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS204)。復号できなかった場合、コントローラ1420は認証データ不受理の出力をデータバスBS3および端子1201を介して携帯電話機100のメモリアンタフェース1200へ出力する(ステップS206)。認証データが復号できた場合、コントローラ1420は、取得した証明書Crtf1がメモリ1415から読出した禁止クラスリストデータに含まれるか否かを判断する(ステップS205)。この場合、証明書Crtf1にはIDが付与されており、コントローラ1420は、受理した証明書Crtf1のIDが禁止クラスリストデータの中に存在するか否かを判別する。証明書Crtf1が禁止クラスリストデータに含まれると判断されると、コントローラ1420は認証データ不受理の出力をデータバスBS3および端子1201を介して携帯電話機100のメモリアンタフェース1200へ出力する(ステップS206)。

【0124】

ステップS204において認証データが公開認証鍵KPmaで復号できなかったとき、およびステップS205において受理した証明書Crtf1が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機100のコントローラ1106は、メモリアンタフェース1200を介して認証データ不受理の出力を受けると、認証データ不受理のため、再生

不能であることをディスプレイ1110に表示する（ステップS207）。

【0125】

ステップS205において、証明書Crtf1が禁止クラスリストデータに含まれていないと判断されると、図12を参照して、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる（ステップS208）。そして、暗号化処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kp1によって暗号化した{Ks2}Kp1をデータバスBS3へ出力する（ステップS209）。そうすると、コントローラ1420は、端子1201を介してメモリインタフェース1200へ{Ks2}Kp1を出力し、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して{Ks2}Kp1を取得する。そして、Kp1保持部1204は、秘密復号鍵Kp1を復号処理部1206へ出力する。

【0126】

復号処理部1206は、Kp1保持部1204から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキーKs2を暗号化処理部1208へ出力する（ステップS210）。そうすると、セッションキー発生部1210は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号化処理部1208へ出力する（ステップS211）。暗号化処理部1208は、セッションキー発生部1210からのセッションキーKs3を復号処理部1206からのセッションキーKs2によって暗号化して{Ks3}Ks2を出力し、コントローラ1106は、データバスBS2およびメモリインタフェース1200を介して{Ks3}Ks2をメモリカード110へ出力する（ステップS212）。

【0127】

メモリカード110の復号処理部1412は、端子1201およびデータバスBS3を介して{Ks3}Ks2を入力し、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3}Ks2を復号して、携帯電話機100で発生されたセッションキーKs3を取得する（ステップS21

3)。

【0128】

セッションキーKs3の受理に応じて、コントローラ1420は、ライセンス情報保持部1440内の対応するアクセス制限情報AC1を確認する（ステップS214）。

【0129】

ステップS214においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数に制限がある場合にはアクセス制限情報AC1のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップS215）。一方、アクセス制限情報AC1によって再生回数が制限されていない場合においては、ステップS215はスキップされ、アクセス制限情報AC1は更新されることなく処理が次のステップ（ステップS216）に進行される。

【0130】

また、ライセンス情報保持部1440内にリクエスト曲の当該コンテンツIDが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【0131】

ステップS214において、当該再生動作において再生が可能であると判断された場合には、メモリに記録された再生リクエスト曲のライセンスキーKcを含むライセンスの復号処理が実行される。具体的には、コントローラ1420の指示に応じて、メモリ1415からデータバスBS4に読出された暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1を復号処理部1422がメモリカード110固有の秘密復号鍵Km1によって復号し、再生処理に必要なライセンスキーKcと再生回路制御情報AC2がデータバスBS4上に得られる（ステップS216）。

【0132】

得られたライセンスキーKcと再生回路制御情報AC2は、切換スイッチ14

44の接点Pdを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点Pdを介して復号処理部1412より受けたセッションキーKs3によってデータバスBS4から受けたライセンスキーKcと再生回路制御情報AC2とを暗号化し、{Kc//AC2}Ks3をデータバスBS3に出力する(ステップS217)。

【0133】

データバスBS3に出力された暗号化データは、メモリインタフェース1200を介して携帯電話機100に送出される。

【0134】

携帯電話機100においては、メモリインタフェース1200を介してデータバスBS2に伝達される暗号化データ{Kc//AC2}Ks3を復号処理部1212によって復号処理を行ない、ライセンスキーKcおよび再生回路制御情報AC2を受理する(ステップS218)。復号処理部1212は、ライセンスキーKcを復号処理部1214に伝達し、再生回路制御情報AC2をデータバスBS2に出力する。

【0135】

コントローラ1106は、データバスBS2を介して、再生回路制御情報AC2を受理して再生の可否の確認を行なう(ステップS219)。

【0136】

ステップS219においては、再生回路制御情報AC2によって再生不可と判断される場合には、再生動作は終了される。

【0137】

ステップS219において再生可能と判断された場合、コントローラ1106は、メモリインタフェース1200を介してメモリカード110に暗号化コンテンツデータ{Data}Kcを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{Data}Kcを取得し、データバスBS3および端子1201を介してメモリインタフェース1200へ出力する(ステップS220)。

【0138】

携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して暗号化コンテンツデータ {Data} Kcを取得し、データバスBS2を介して暗号化コンテンツデータ {Data} Kcを復号処理部1214へ与える。そして、復号処理部1214は、暗号化コンテンツデータ {Data} Kcを復号処理部1212から出力されたコンテンツキーKcによって復号してコンテンツデータDataを取得する（ステップS221）。

【0139】

そして、復号されたコンテンツデータDataは音楽再生部1216へ出力され、音楽再生部1216は、コンテンツデータを再生し、DA変換器1218はデジタル信号をアナログ信号に変換して端子1220へ出力する。そして、スイッチ1222は端子1220を選択して音楽データは端子1224を介してヘッドホン130へ出力されて再生される（ステップS222）。これによって再生動作が終了する。

【0140】

携帯電話機100のユーザ1は、携帯電話機100を用いて配信サーバ30から暗号化コンテンツデータ {Data} KcとライセンスキーKcとをメモリカード110に受信し、ライセンスキーKcによって暗号化コンテンツデータ {Data} Kcを復号して再生することができる。

【0141】

なお、ユーザ1の携帯電話機100は、ユーザ2の携帯電話機100から暗号化コンテンツデータ {Data} Kcを転送してもらう（受信する）こともできる。この場合、受信した暗号化コンテンツデータ {Data} Kcを復号するためのライセンスキーKcがメモリカード110に記録されていないことを確認すると、配信サーバ30へライセンスキーKcの配信を要求する。

【0142】

同様に、配信サーバからライセンスキーを受信してそのライセンスキーにより暗号化コンテンツデータを復号して再生することができる。

【0143】

次に、第1の実施の形態による携帯電話機100におけるシェル型筐体の開閉

状態とコンテンツデータのダウンロード処理との関係を、図 1 3 を参照して詳しく説明する。

【0 1 4 4】

まず、携帯電話機 1 0 0 は、シェル型筐体が開いた状態であり、かつ待ち受け状態であるとする（ステップ S 1 0 0 0）。この状態で、要求するコンテンツデータをメモリカード 1 1 0 に記録するダウンロード処理が指定されたか否かが判断される（ステップ S 1 0 0 2）。ダウンロード処理が指定された場合、配信要求の正当性が確認されたことを条件に、携帯電話機 1 0 0 はダウンロード状態、すなわち通話状態になる（ステップ S 1 0 0 4）。ダウンロード処理でなく他の処理モードが指定された場合（再生モード等）には、当該他のモードに移る（ステップ S 1 0 0 6）。

【0 1 4 5】

配信されるデータ量等をコントローラ 1 1 0 6 で監視することにより、ダウンロードが終了したか否かが判断される（ステップ S 1 0 0 8）。

【0 1 4 6】

ダウンロードが終了したと判断されると、再び待ち受け状態（ステップ S 1 0 0 0）に移る。

【0 1 4 7】

ダウンロードが未終了であると判断されると、シェル開閉検出部 1 1 1 7 により、携帯電話機 1 0 0 のシェル型筐体が閉じられたか否かが判断される（ステップ S 1 0 1 0）。

【0 1 4 8】

シェル型筐体が開いた状態であると判断されると、ダウンロード状態を継続する（ステップ S 1 0 0 4）。

【0 1 4 9】

シェル型筐体が閉じた状態であると判断されると、現在のダウンロードが終了するまでダウンロード処理を継続する状態（ダウンロード終了待ち状態）に移る（ステップ S 1 0 1 2）。ダウンロード終了待ち状態では、電源制御部 1 1 1 6 により、通話に必要な電源電圧が各回路に継続して供給される。

【0150】

そして、配信されるデータ量等をコントローラ1106で監視することにより、ダウンロードが終了したか否かが判断される（ステップS1014）。

【0151】

ダウンロードが未終了であると判断されると、前述したダウンロード終了待ち状態に移る（ステップS1012）。

【0152】

ダウンロードが終了したと判断されると、通話が切断される（ステップS1016）。

【0153】

そして、シェル型筐体が閉じた状態での待ち受け状態になる。この時、電源制御部1116により、携帯電話機100は、最も消費電力が低い低消費電力モードに移る。

【0154】

次に、第1の実施の形態による携帯電話機100におけるシェル型筐体の開閉状態とデータ再生処理との関係を、図14を参照して詳しく説明する。メモリカード110に再生するコンテンツデータがすでに記録されている状態とする。

【0155】

まず、携帯電話機100は、シェル型筐体が開いた状態にあり、待ち受け状態であるとする（ステップS1100）。この状態で、コンテンツデータを再生する再生モードが指定されたか否かが判断される（ステップS1102）。再生モードが指定された場合、携帯電話機100は指定したコンテンツデータを再生する再生状態になる（ステップS1104）。再生モードではなく他の処理モードが指定された場合（ダウンロード等）には、当該他のモードに移る（ステップS1106）。

【0156】

再生処理に入ると、コントローラ1106により、再生が終了したか否かが判断される（ステップS1108）。

【0157】

再生が終了したと判断されると、再び待ち受け状態（ステップ S 1 1 0 0）に移る。

【 0 1 5 8 】

再生が未終了であると判断されると、シェル開閉検出部 1 1 1 7 により、携帯電話機 1 0 0 のシェル型筐体が閉じられたか否かが判断される（ステップ S 1 1 1 0）。

【 0 1 5 9 】

シェル型筐体が開いた状態であると判断されると、再生状態を継続する（ステップ S 1 1 0 4）。

【 0 1 6 0 】

シェル型筐体が閉じた状態であると判断されると、コンテンツデータの再生が終了するまで再生処理を継続する状態（再生終了待ち状態）に移る（ステップ S 1 1 1 2）。再生終了待ち状態では、電源制御部 1 1 1 6 により、再生処理に必要な電源電圧が各回路に継続して供給される。

【 0 1 6 1 】

そして、コントローラ 1 1 0 6 により、再生が終了したか否かが判断される（ステップ S 1 1 1 4）。

【 0 1 6 2 】

再生が未終了であると判断されると、前述した再生終了待ち状態に移る（ステップ S 1 1 1 2）。

【 0 1 6 3 】

再生が終了したと判断されると、シェル型筐体が閉じた状態での待ち受け状態になる。この時、電源制御部 1 1 1 6 により、携帯電話機 1 0 0 は、最も消費電力が低い低消費電力モードに移る。

【 0 1 6 4 】

第 1 の実施の形態によれば、携帯電話機は、暗号化コンテンツデータの著作権を十分に保護しながら再生することができる。

【 0 1 6 5 】

また、ダウンロード中にシェル型筐体を閉じても、携帯電話機 1 0 0 はダウン

ロードを完了させることができる。特に、音楽コンテンツ等の大量のデータをダウンロードする場合、シェル型筐体を開けた状態で放置する必要がなくなる。また、再生中にシェル型筐体を閉じて、携帯電話機 1 0 0 は音楽再生を継続させることができる。

【0 1 6 6】

〔実施の形態 2〕

第 2 の実施の形態では、第 1 の実施の形態の携帯電話機 1 0 0 の他の構成例を示す。なお、データ配信システム、ライセンスサーバ、メモリカードの構成については第 1 の実施の形態で説明したとおりである。

【0 1 6 7】

第 2 の実施の形態による携帯電話機は、通信処理系回路と再生系とを分離するように回路を構成する。具体的には、通信機能を有する携帯電話機本体は図 1 5 に示す回路構成とする（携帯電話機本体 1 0 0 a と称す）。そして、携帯電話機本体 1 0 0 a と分離した状態で、図 1 6 に示す音楽再生モジュール 1 2 0 を形成する。コントローラ 1 1 0 6 は、携帯電話機本体 1 0 0 a のメイン CPU 1 1 0 6 a と音声再生モジュール 1 2 0 のサブ CPU 1 2 3 0 とに分離される形となる。

【0 1 6 8】

携帯電話機本体 1 0 0 a および音声再生モジュール 1 2 0 は、ともに上述したシェル型筐体に内蔵される。リモコン型のように分離した形態であってもよい（その場合、図 1 6 に示すリモコン制御部 1 2 2 2 のような、キー操作部 1 2 2 4 およびディスプレイ 1 2 2 6 が実装されてもよい）。

【0 1 6 9】

図 1 5 を参照して、携帯電話機本体 1 0 0 a は、アンテナ 1 1 0 2 と、送受信部 1 1 0 4 と、データバス B S 2 と、データバス B S 2 を介して携帯電話機本体 1 0 0 a の回路動作を制御するためのメイン CPU 1 1 0 6 a と、キー操作部 1 1 0 8 と、ディスプレイ 1 1 1 0 と、音声再生部 1 1 1 2 と、D A 変換器 1 1 1 3 と、D A 変換器の出力を受ける端子 1 1 1 4 とを含む。

【0 1 7 0】

携帯電話機本体100aはさらに、電源制御部1116と、シェル開閉検出部1117と、シリアルインタフェース1118とを含む。シリアルインタフェース1118を介して、携帯電話機本体100aは、音声再生モジュール120との間でデータの授受を行う。

【0171】

シェル開閉検出部1117は上述したように、携帯電話機本体100aと音声再生モジュール120とを包むシェル型筐体が閉じられた状態か開かれた状態かを検出する。検出結果は、データバスBS2を介してメインCPU1106aに転送される。電源制御部1117は、メインCPU1106aの制御に基づき、携帯電話機本体100aまたは／および音声再生モジュール1120に動作電源を供給する。

【0172】

図16を参照して、音声再生モジュール120は、認証データ保持部1202と、Kp1保持部1204と、復号処理部1206、1212、1214と、暗号化処理部1208と、セッションキー発生部1210と、音楽再生部1216と、DA変換器1218と、接続端子1220とを含む。

【0173】

音声再生モジュール120はさらに、データバスBS3と、音声再生モジュール120の動作を制御するサブCPU1230と、メモリカード110と、メモリカード110とデータバスBS3との間に配置されるメモリインタフェース1200とを含む。シリアルインタフェース1228を介して、音声再生モジュール120は、携帯電話機100aとの間でデータの授受を行う。

【0174】

シェル型筐体の開閉状態とコンテンツデータのダウンロード処理との関係は、第1の実施の形態で説明したとおりである。また、シェル型筐体の開閉状態とコンテンツデータの再生処理との関係は、第1の実施の形態で説明したとおりである。

【0175】

このように、第2の実施の形態による携帯電話機（通信処理系と再生処理系と

を分離した形態)であっても、第1の実施の形態と同様の効果を有する。

【0176】

〔実施の形態3〕

図17および図18を参照して、第3の実施の形態について説明する。携帯電話機100は、他の携帯電話機100に装着されたメモリカード110から新たな暗号化コンテンツデータ {Data} Kcを受信することができる。この際、暗号化コンテンツデータ {Data} Kcに対応するコンテンツキーKcの配信要求を配信サーバ30へ行なう。第3の実施の形態においては、携帯電話機100は、コンピュータを用いてインターネット配信等された暗号化コンテンツデータ {Data} Kcを受信してメモリカード110に記録し、その暗号化コンテンツデータ {Data} Kcに対応するコンテンツキーKcの配信要求を配信サーバ30に対して行なう場合について説明する。

【0177】

図17を参照して、コンピュータ140を用いた暗号化コンテンツデータ {Data} Kcの配信について説明する。携帯電話機100にはメモリカード110が着脱可能であり、音楽を再生するためのヘッドホン130が接続されている。そして、携帯電話機100は、通信ケーブル145を介してコンピュータ140と接続されている。

【0178】

コンピュータ140は、ハードディスク141と、コントローラ142と、外部インタフェース143とを備える。そして、ハードディスク141はデータバスBS5を介してコントローラ142と接続され、コントローラ142はライセンス保護モジュール144を含む。

【0179】

ハードディスク141は、インターネット配信によってコンピュータ140に配信された暗号化コンテンツデータ {Data} KcをデータバスBS5を介して記憶する。コントローラ142は、携帯電話機100のユーザ1から通信ケーブル145および外部インタフェース143を介して暗号化コンテンツデータ {Data} Kcの送信要求があると、ハードディスク141から暗号化コンテン

ツデータ {D a t a} K c を読出し、外部インタフェース 1 4 3 を介して外部へ出力する。

【0 1 8 0】

外部インタフェース 1 4 3 は、携帯電話機 1 0 0 から通信ケーブル 1 4 5 を介してコンピュータ 1 4 0 に入力された信号をコントローラ 1 4 2 に入力するとともに、コントローラ 1 4 2 からの信号を外部へ出力する。

【0 1 8 1】

ライセンス保護モジュール 1 4 4 は、図 6 に示すデータ処理部 3 1 0 と同じ構成を有し、携帯電話機 1 0 0 に装着されたメモリカード 1 1 0 に暗号化コンテンツデータ {D a t a} K c を送信するために、上述したように携帯電話機 1 0 0 およびメモリカード 1 1 0 と公開暗号鍵、セッションキー等のやり取りを行ないながら、暗号化コンテンツデータ {D a t a} K c を保護してメモリカード 1 1 0 へ送信するものである。

【0 1 8 2】

インターネット配信によって配信サーバからコンピュータ 1 4 0 に暗号化コンテンツデータ {D a t a} K c が配信され、コンピュータ 1 4 0 のハードディスク 1 4 1 にデータバス B S 5 を介して暗号化コンテンツデータが記憶されている。

【0 1 8 3】

携帯電話機 1 0 0 のユーザ 1 がキー操作部 1 1 0 8 から送信要求を入力すると、通信ケーブル 1 4 5 および外部インタフェース 1 4 3 を介して送信要求がコントローラ 1 4 2 に入力される。コントローラ 1 4 2 は、送信要求を受付けると、要求された暗号化コンテンツデータ {D a t a} K c をデータバス B S 5 を介してハードディスク 1 4 1 から読出し、ライセンス保護モジュール 1 4 4 に入力する。

【0 1 8 4】

ライセンス保護モジュール 1 4 4 は、上述したようにメモリカード 1 1 0 と通信ケーブル 1 4 5 を介して公開暗号鍵、セッションキー等のやり取りを行ない、暗号化コンテンツデータ {D a t a} K c をメモリカード 1 1 0 へ送信する。

【0185】

送信後、携帯電話機100のユーザ1は、上述したのと同じ方法によって暗号化コンテンツデータ {Data} KcのコンテンツキーKcを配信サーバから配信してもらい、暗号化コンテンツデータ {Data} Kcを再生する。

【0186】

また、コンピュータ140は、インターネット配信によって暗号化コンテンツデータ {Data} Kcを受信しなくても良く、暗号化コンテンツデータ {Data} Kcが記録されたCD-ROMをコンピュータ140に接続されたCD-ROMドライブ（図示せず）に装着し、そのCD-ROMから暗号化コンテンツデータ {Data} Kcを読み出してメモリカード110へ送信しても良い。この場合、CD-ROMに記録された暗号化コンテンツデータ {Data} Kcを、一旦、ハードディスク141に記憶しておいても良い。

【0187】

さらに、コンピュータ140は、CDリッピングによって暗号化コンテンツデータ {Data} Kcを生成しても良い。リッピングとは、音楽CDから取得した音楽データを、音楽再生モジュールで再生できるように変換することを言う。まず、取得した音楽データに対してライセンスを生成する。次いで、取得した音楽データを音楽再生部1216にて再生可能なコンテンツデータに変換した後、生成したライセンスに含まれるコンテンツキーにて復号可能な暗号化を行なうもので、リッピングによって得られた暗号化コンテンツデータの生成されたライセンスには、複製ができないように管理される。したがって、音楽CDからの1次複製であるCDリッピングは、コンテンツの暗号化と、その復号鍵であるコンテンツキーを含むライセンスが複製できない構成を取ることで著作権を保護した適法な行為である。

【0188】

CDを用いた場合、音楽CDから取得して生成した暗号化コンテンツデータ {Data} Kcは、一旦、ハードディスク141に記録してからメモリカード110へ送信しても良いし、ハードディスク141に送信せずに、直接、メモリカード110へ送信しても良い。

【0189】

暗号化コンテンツデータ {Data} Kc は、図18に示すようにメモ리카ード110を、直接、コンピュータ140に装着してメモ리카ード110に暗号化コンテンツデータ {Data} Kc を記録しても良い。この場合、コンピュータ140のコントローラ142は、ライセンス保護モジュール144によって、直接、メモ리카ード110に暗号化コンテンツデータを記録する。

【0190】

図18においても、コンピュータ140は、図17に示す場合と同じ方法により暗号化コンテンツデータ {Data} Kc を取得する。

【0191】

携帯電話機100が、新たに受信した暗号化コンテンツデータ {Data} Kc に対応するコンテンツキーKc の配信要求を配信サーバ30へ行なう場合のフローチャート、および新たに受信した暗号化コンテンツデータ {Data} Kc を再生するフローチャートは、第1の実施の形態と同じである。

【0192】

第3の実施の形態によれば、携帯電話機は、インターネット配信、およびCDリッピング等によって、新たな暗号化コンテンツデータを受信したとき、その暗号化コンテンツデータを復号するコンテンツキーの配信要求を自動的に配信サーバへ行なうので、携帯電話機のユーザは暗号化コンテンツデータのみをインターネット配信等によって受信したときでも、その暗号化コンテンツデータを再生することができる。

【0193】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 (a) ~ (c) は、携帯電話機のシェル型筐体の開閉状態を示す

概念図である。

【図 3】 図 1 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図 4】 図 1 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図 5】 図 1 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。。

【図 6】 ライセンスサーバの構成を示す概略ブロック図である。

【図 7】 携帯電話機の構成を示すブロック図である。

【図 8】 メモリカードの構成を示すブロック図である。

【図 9】 図 1 に示すデータ配信システムにおける配信動作を説明するための第 1 のフローチャートである。

【図 1 0】 図 1 に示すデータ配信システムにおける配信動作を説明するための第 2 のフローチャートである。

【図 1 1】 携帯電話機における再生動作を説明するための第 1 のフローチャートである。

【図 1 2】 携帯電話機における再生動作を説明するための第 2 のフローチャートである。

【図 1 3】 第 1 の実施の形態による携帯電話機 1 0 0 におけるシェル型筐体の開閉状態とダウンロード処理との関係を示すフローチャートである。

【図 1 4】 第 1 の実施の形態による携帯電話機 1 0 0 におけるシェル型筐体の開閉状態と再生処理との関係を示すフローチャートである。

【図 1 5】 第 2 の実施の形態による携帯電話機本体 1 0 0 a の構成を示すブロック図である。

【図 1 6】 第 2 の実施の形態による音声再生モジュール 1 2 0 の構成を示すブロック図である。

【図 1 7】 コンピュータを用いた暗号化コンテンツデータの配信を概念的に説明するための概略図である。

【図 1 8】 コンピュータを用いた暗号化コンテンツデータの配信を概念的

に説明するための他の概略図である。

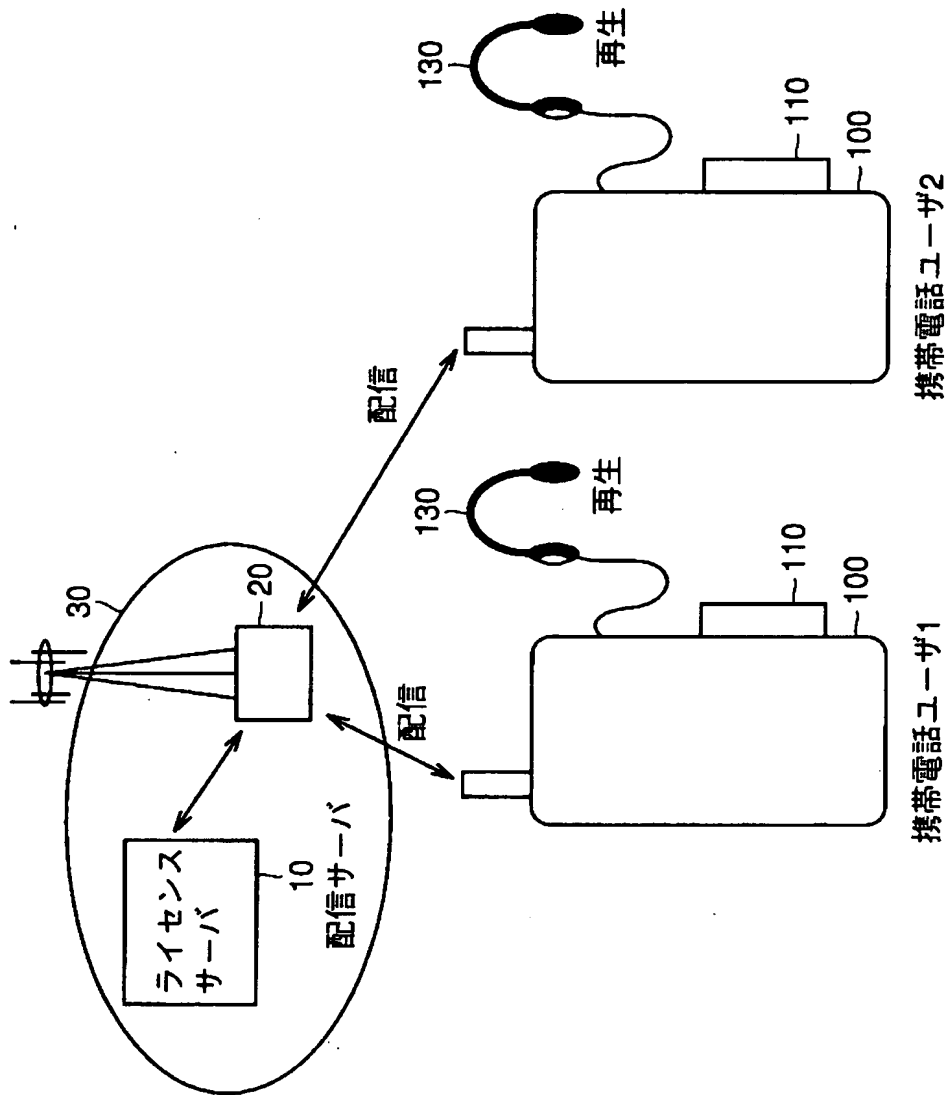
【図19】 従来のシェル型携帯電話機の電源供給に関して説明するためのフローチャートである。

【符号の説明】

10 ライセンスサーバ、20 配信キャリア、30 配信サーバ、100 携帯電話機、110 メモリカード、130 ヘッドホーン、140 コンピュータ、141 ハードディスク、142, 1106, 1420 コントローラ、143 外部インタフェース、144 ライセンス保護モジュール、145 通信ケーブル、302 課金データベース、304 情報データベース、306 CRLデータベース、310 データ処理部、312, 320, 1206, 1212, 1214, 1404, 1408, 1412, 1422 復号処理部、315 配信制御部、316, 1210, 1418 セッションキー発生部、318, 326, 328, 1208, 1410 暗号化処理部、350 通信装置、1102 アンテナ、1104 送受信部、1108, 1110 ディスプレイ、1112 音声再生部、1113, 1218 DA変換器、1114, 1201, 1220, 1224 端子、1116 電源制御部、1117 シェル開閉検出部、1200 メモリインタフェース、1222 スイッチ、1402 Km c1保持部、1414, 1414B KPma保持部、1415 メモリ、1416 KPm1保持部、1421 Km1保持部、1440 ライセンス情報保持部、1442, 1444, 1446 切換スイッチ、1202, 1400 認証データ保持部、1204 Kp1保持部、1216 音楽再生部。

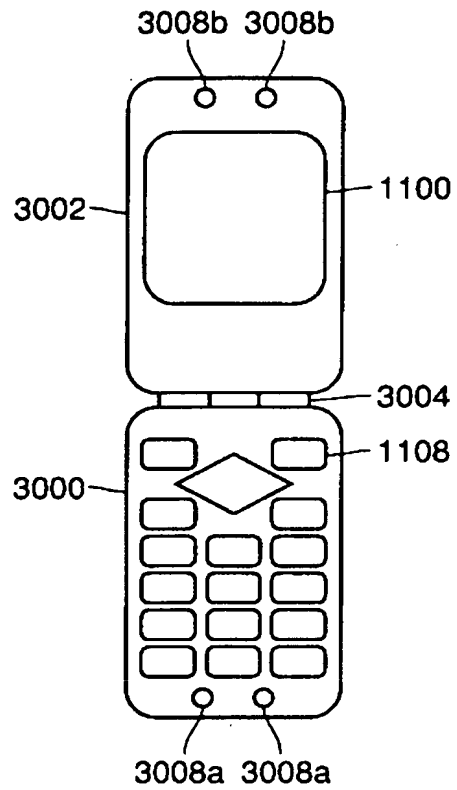
【書類名】 図面

【図 1】

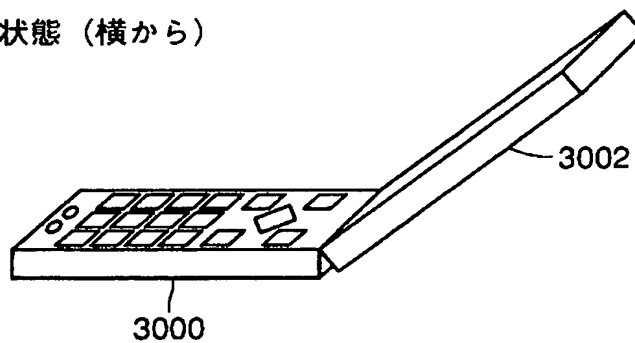


【図 2】

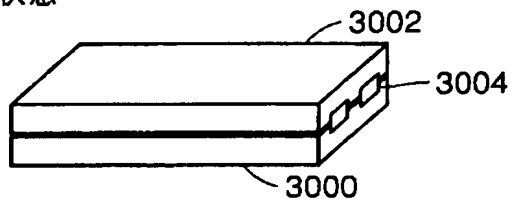
(a) 開いた状態



(b) 開いた状態 (横から)



(c) 閉じた状態



【図 3】

名称	属性	保持／発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータの形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード(コンテンツIDを含めて識別することも可)
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数、機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報(例：再生可否)

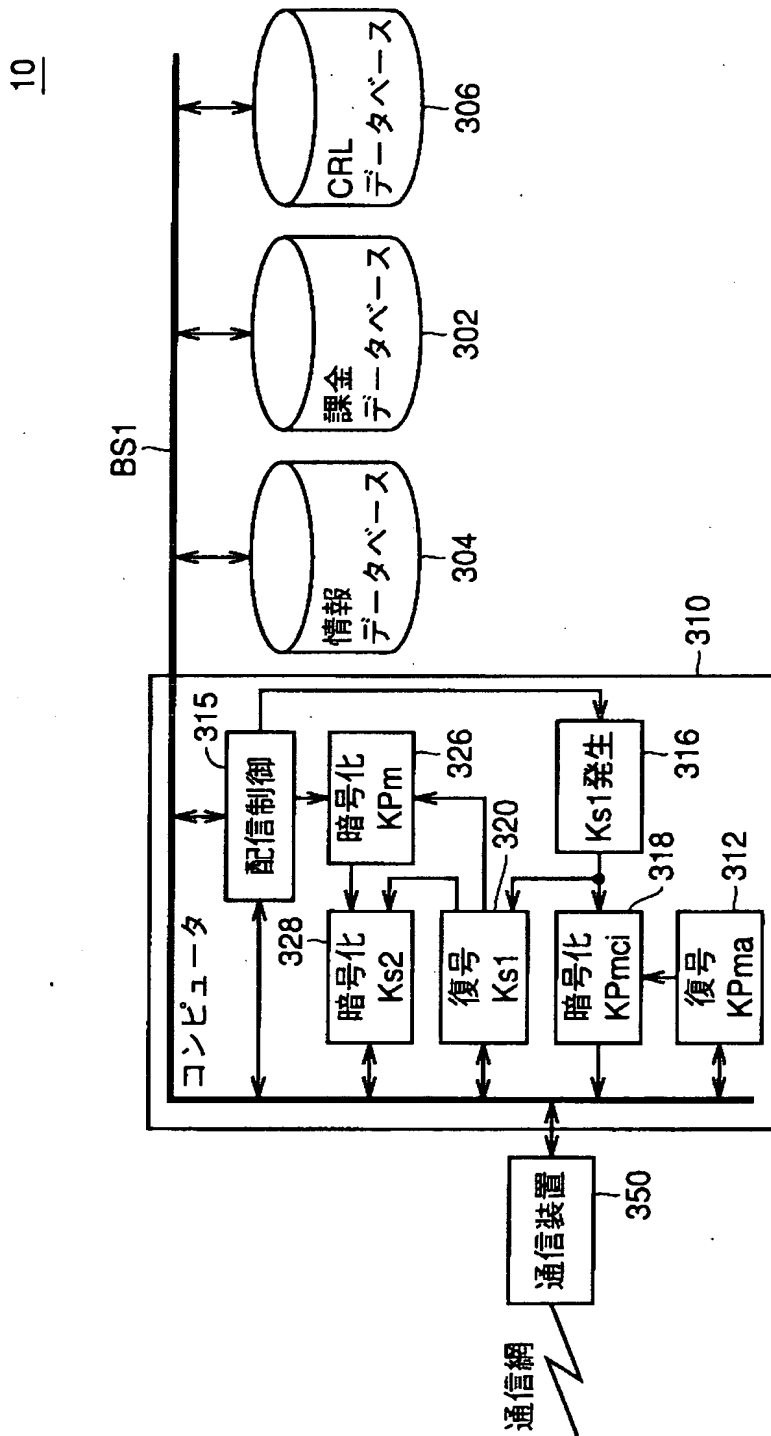
【図 4】

名称	属性	保持／発生箇所	機能・特徴
CRL	禁止クラスリスト 関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報 (差分データ形式)
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵 (非対称鍵)	携帯電話機	Kpnにて復号可能。 {KPpn/Crtfn}KPmaの形式で出荷時に記録 *携帯電話機の種類nごとに異なる。
KPmci	公開暗号鍵 (非対称鍵)	メモリカード	Kmciにて復号可能。 {KPmci/Cmci}KPmaの形式で出荷時に記録 *メモリカードの種類iごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 *携帯電話機の種類nごとに異なる。
Kmci	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 *メモリカードの種類iごとに異なる。
Crtfn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 {KPpn/Crtfn}KPmaの形式で出荷時に記録 *携帯電話機の種類nごとに異なる。
Cmci		メモリカード	メモリカードのクラス証明書。認証機能を有する。 {KPmci/Cmci}KPmaの形式で出荷時に記録 *メモリカードの種類iごとに異なる。

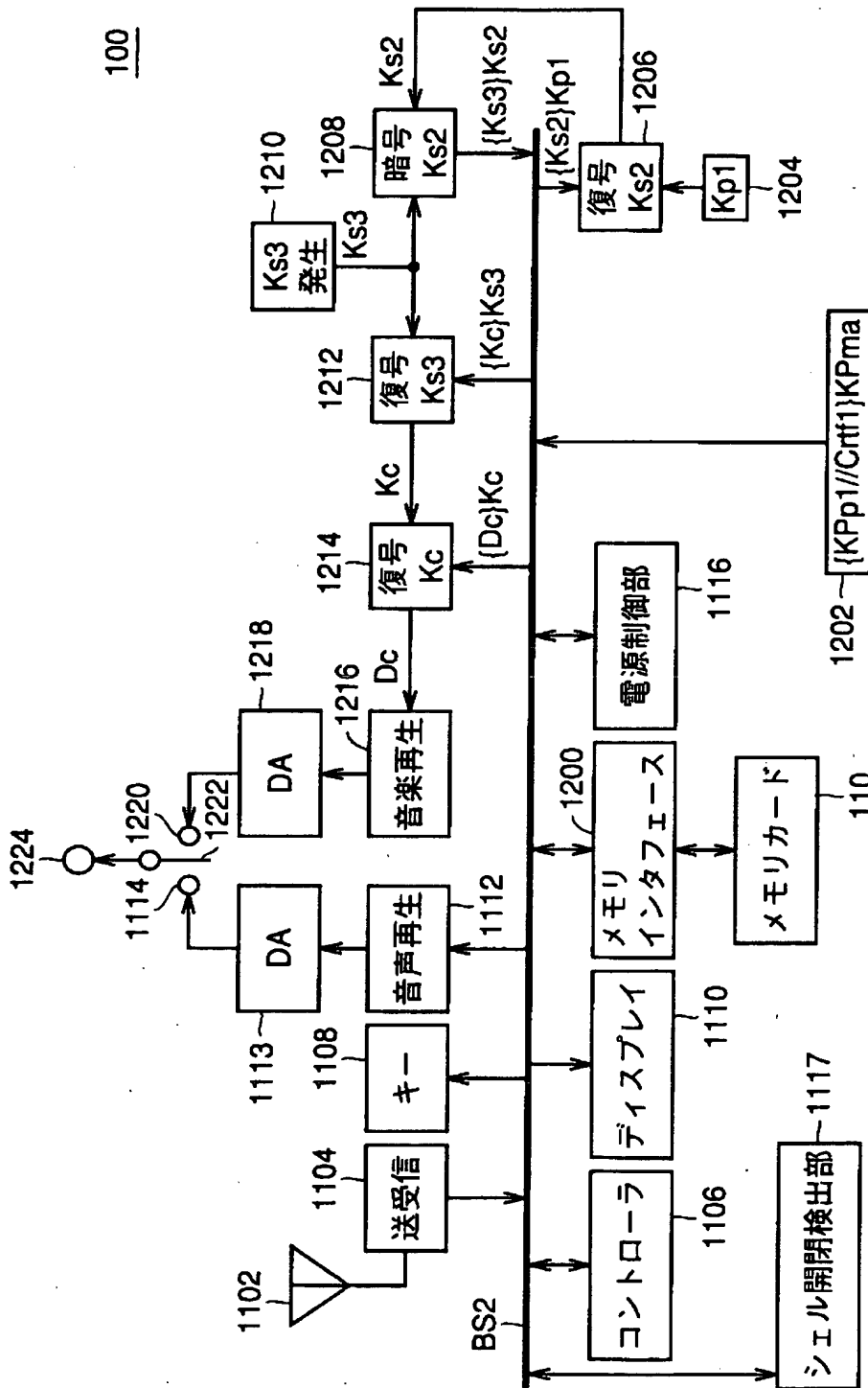
【図 5】

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／再生セッション毎に発生
Ks3		携帯電話機	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 Kpmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵 (非対称鍵)	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。

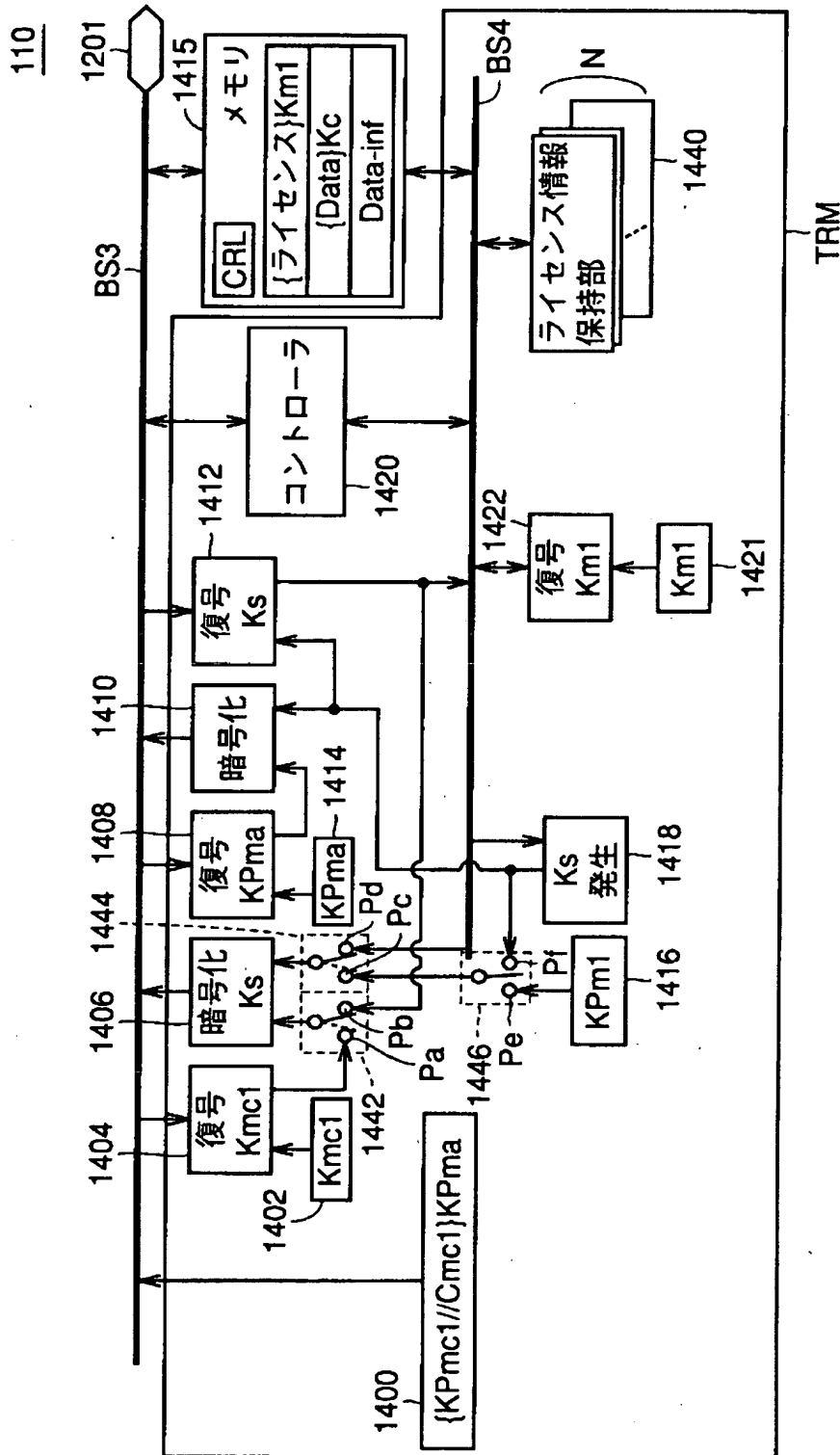
【図 6】



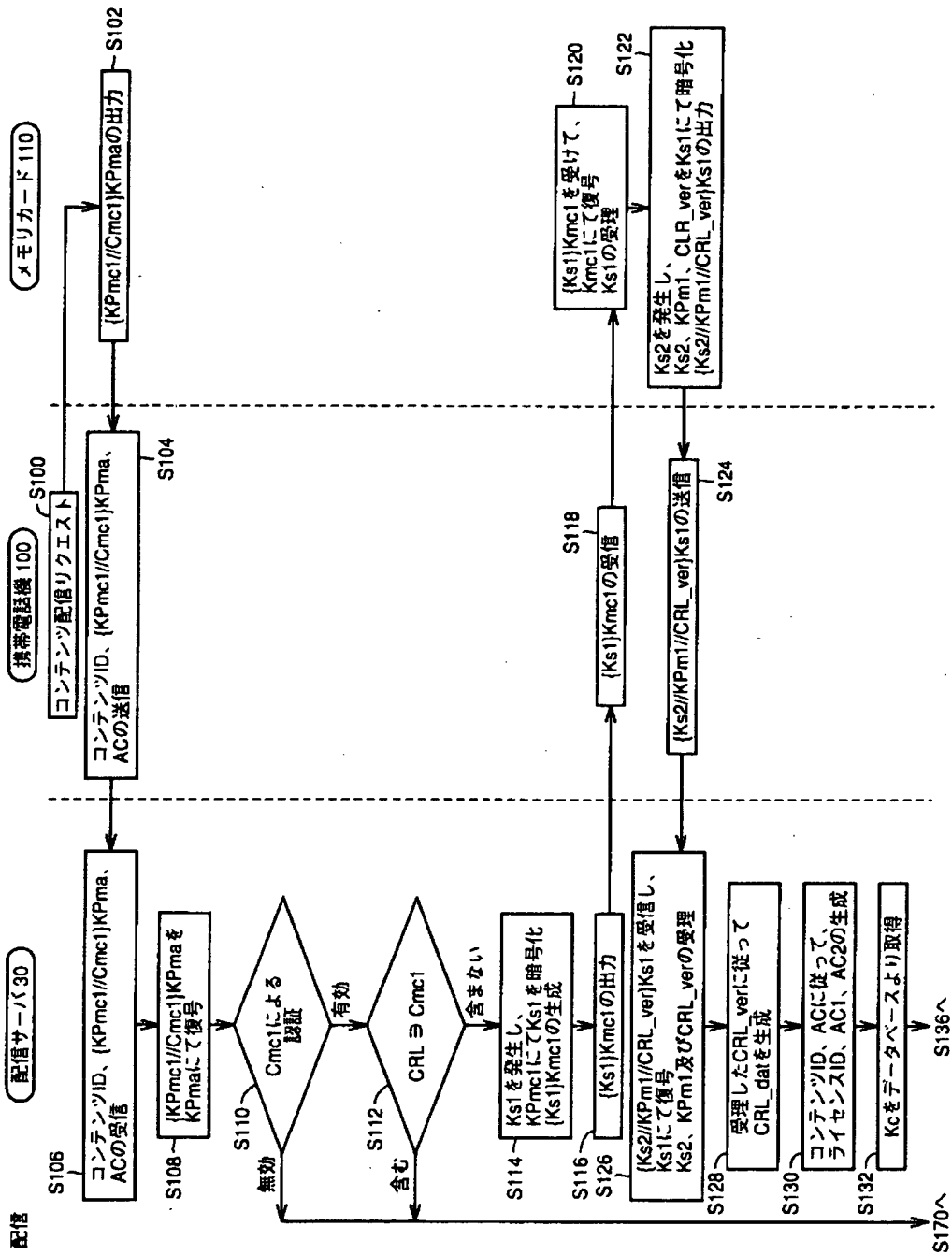
【図 7】



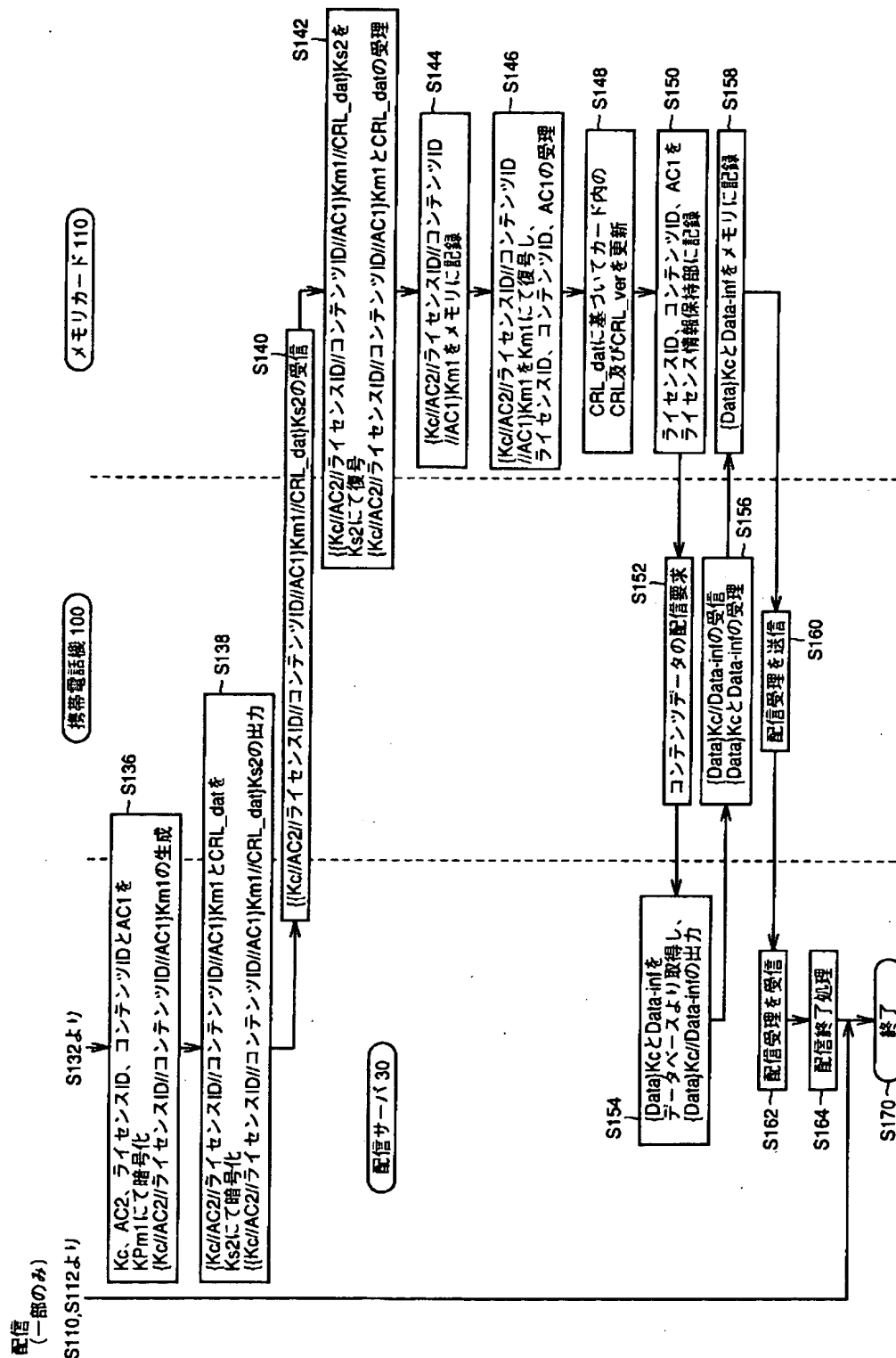
【図 8】



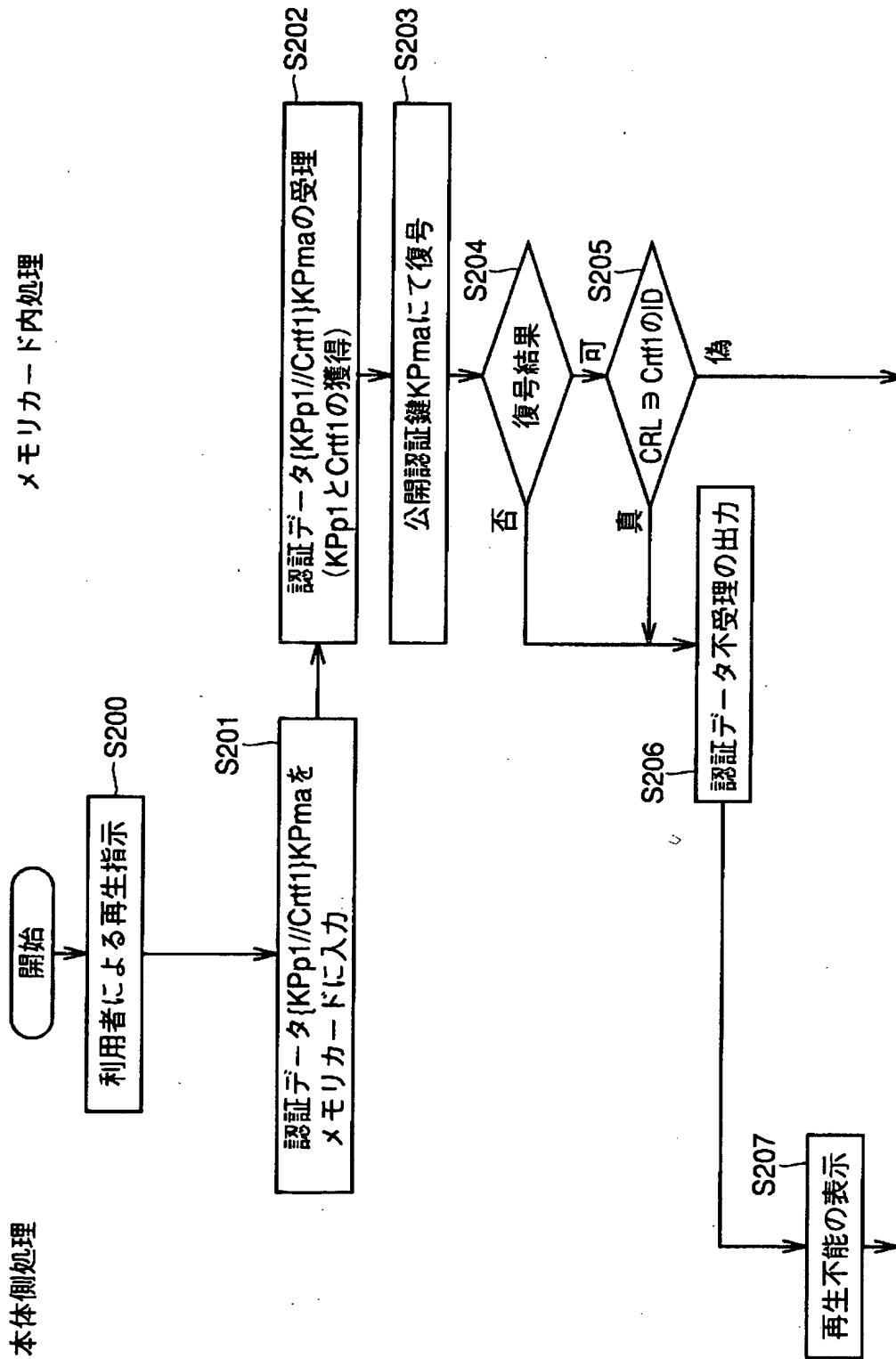
【図 9】



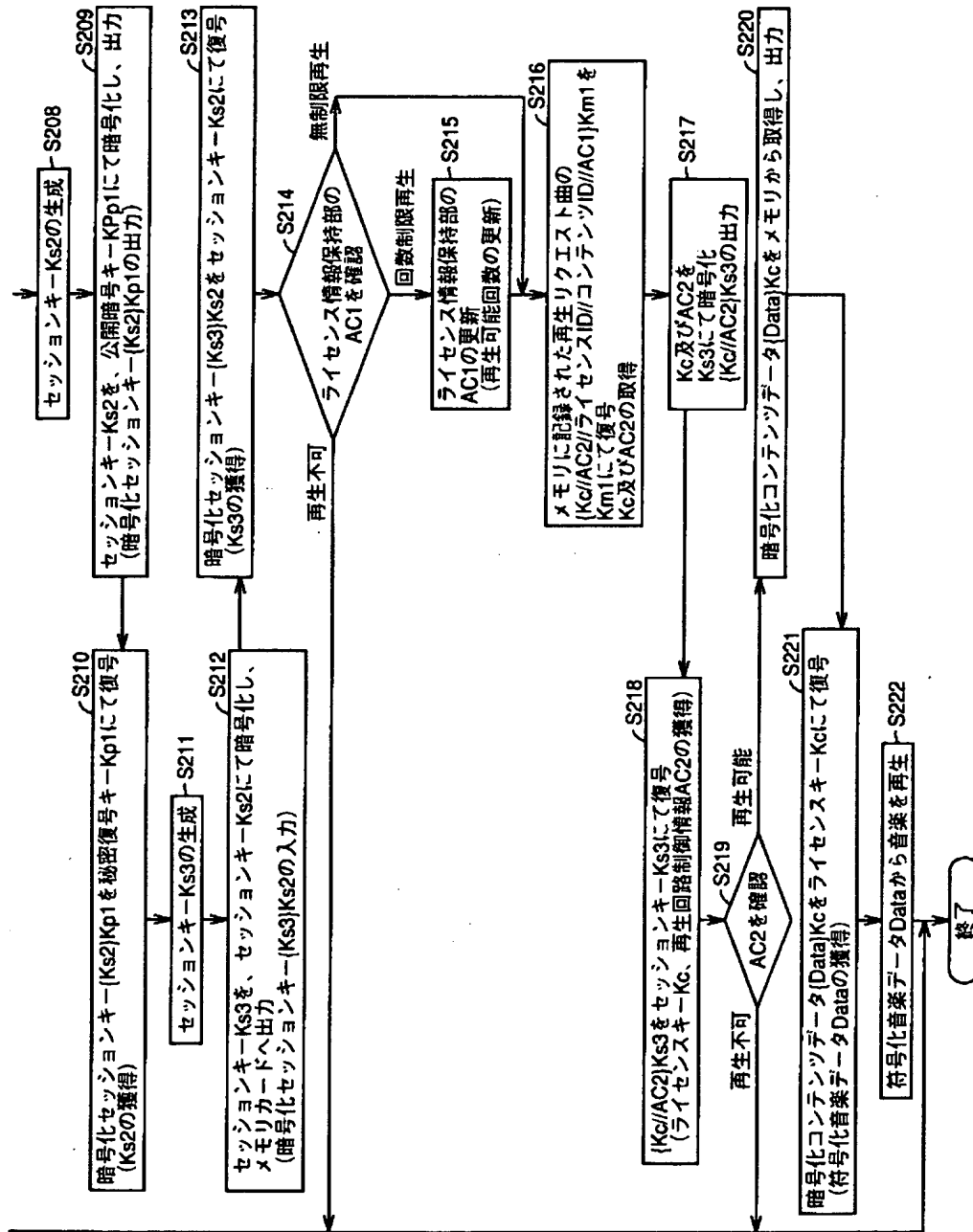
【図 10】



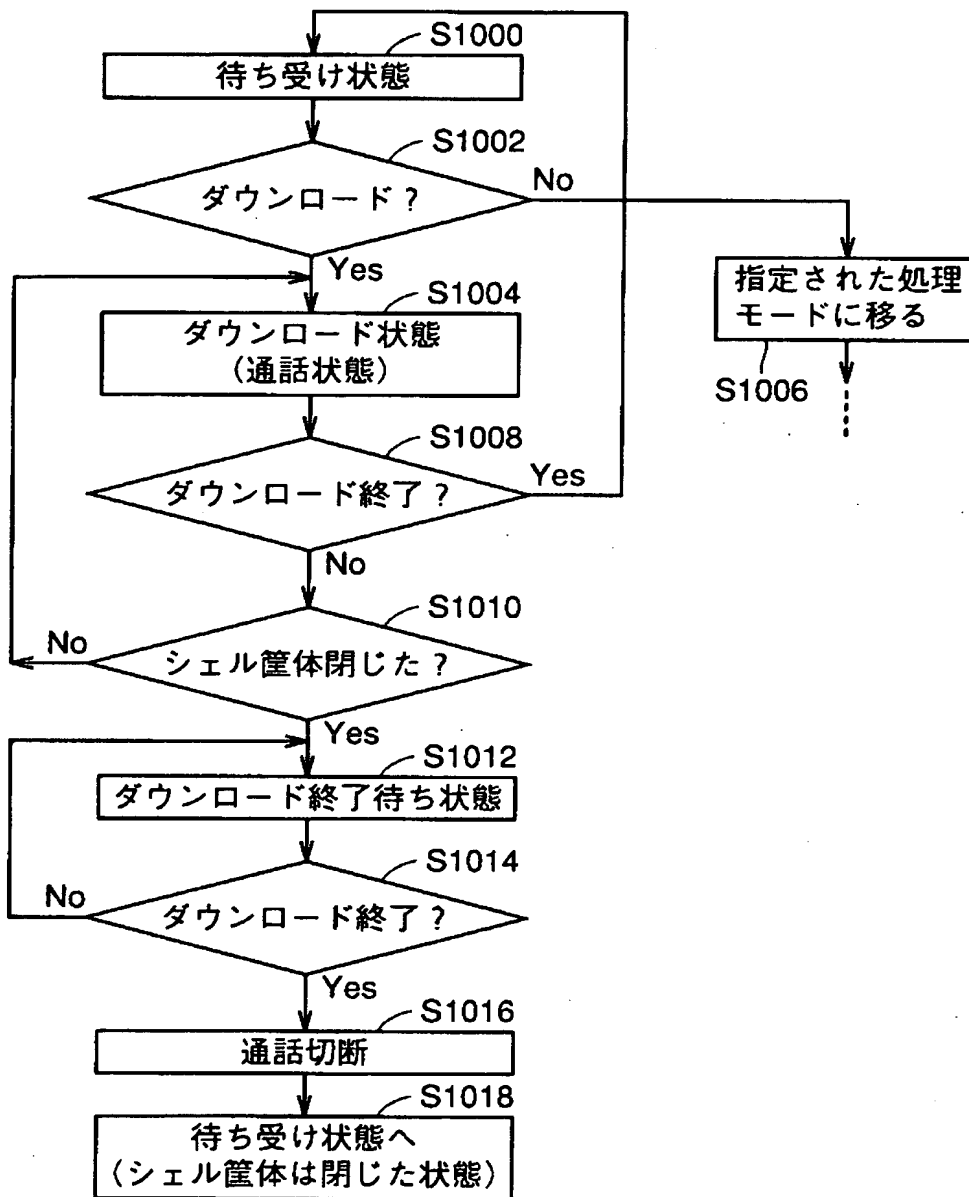
【図 11】



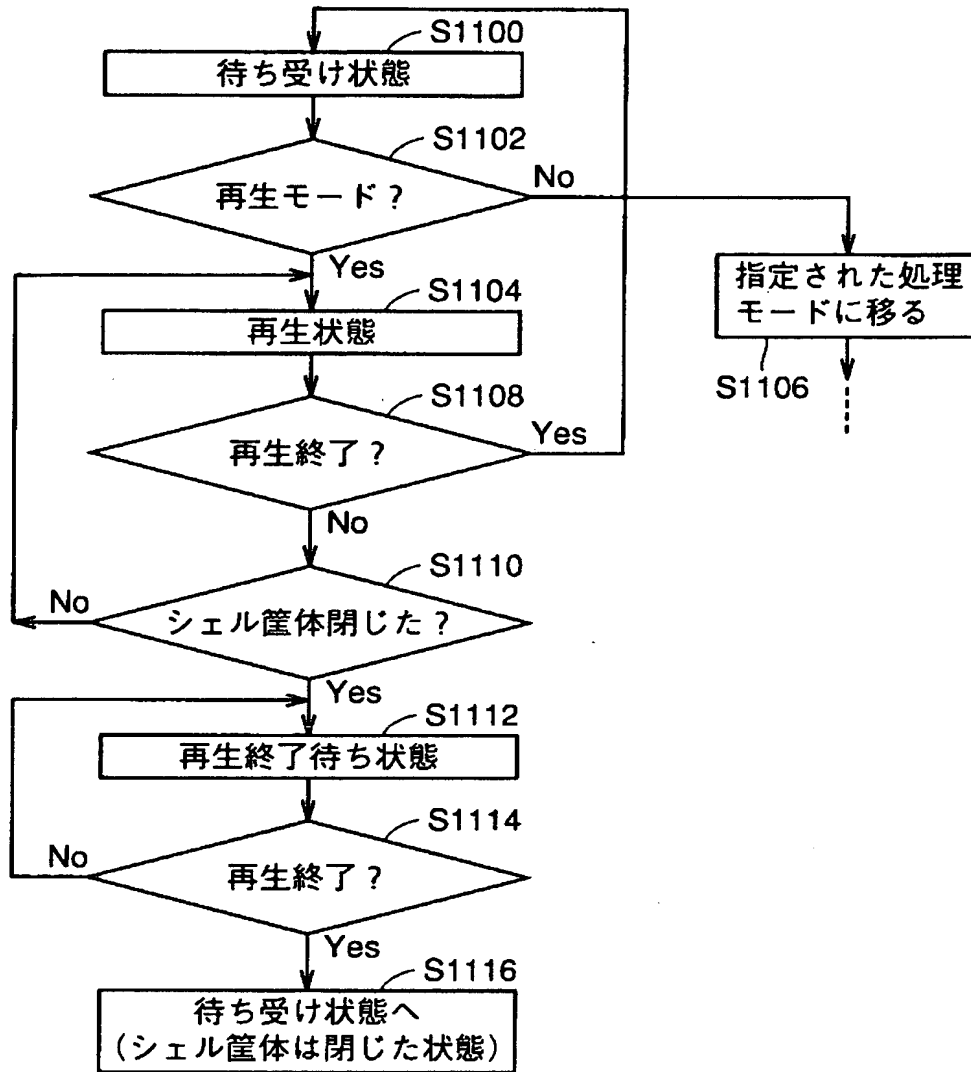
【図 12】



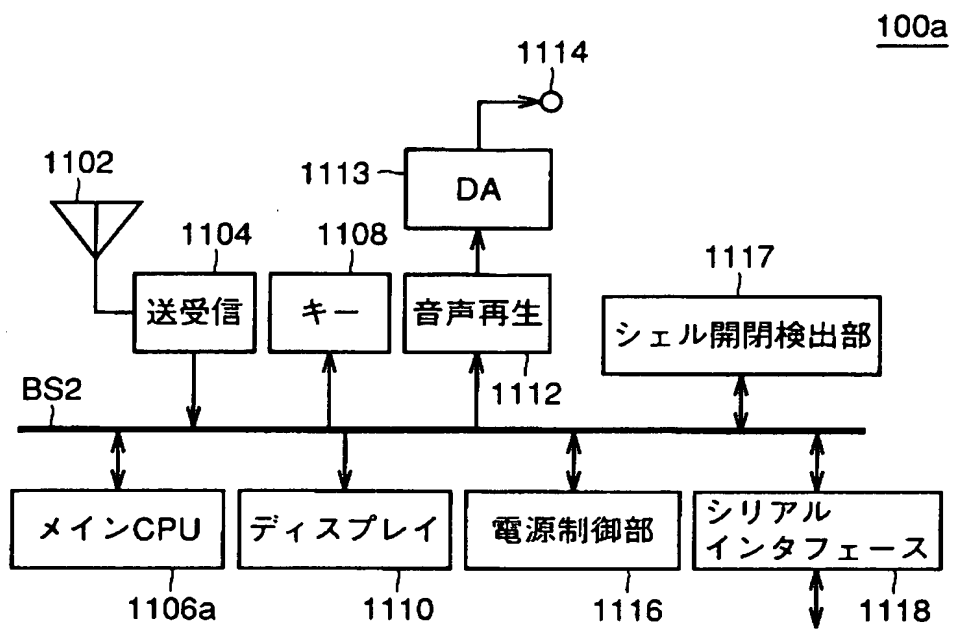
【図13】



【図 1 4】

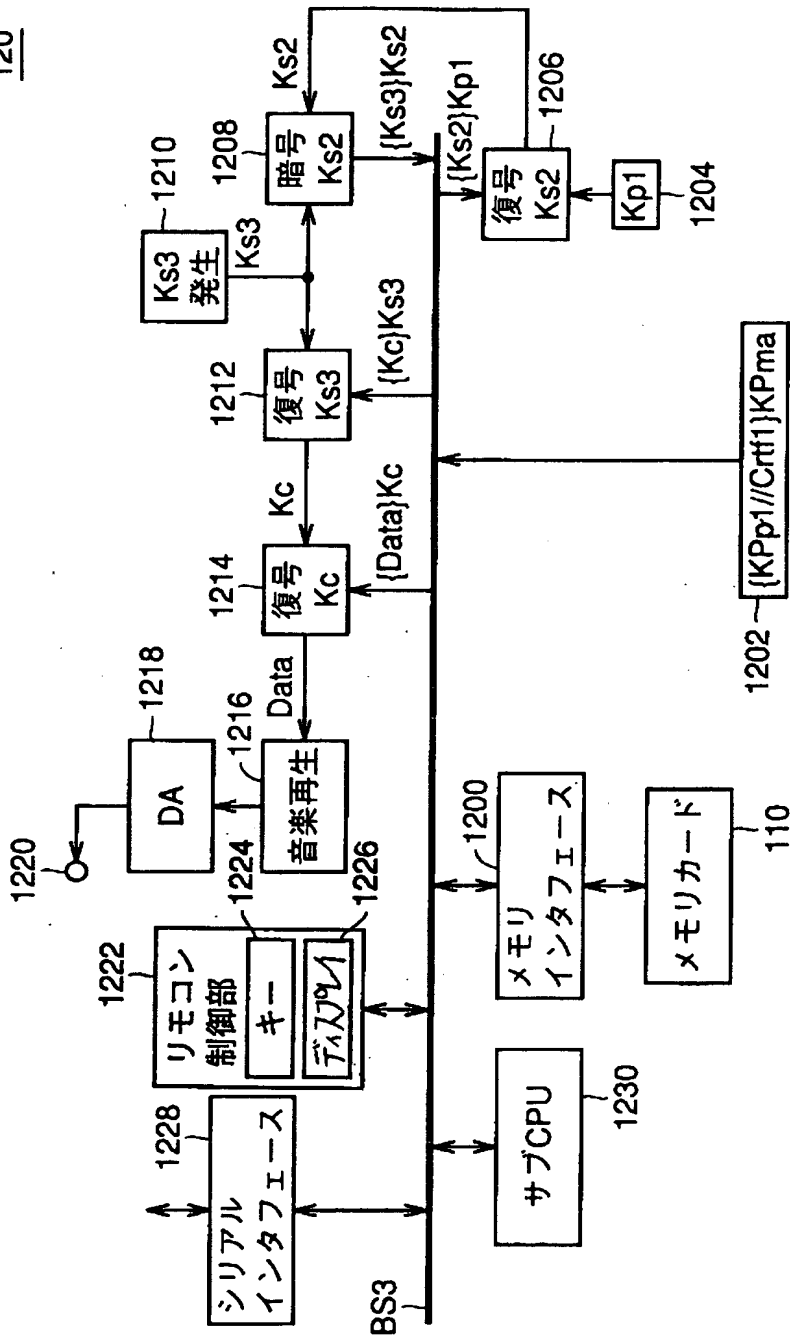


【図 1 5】

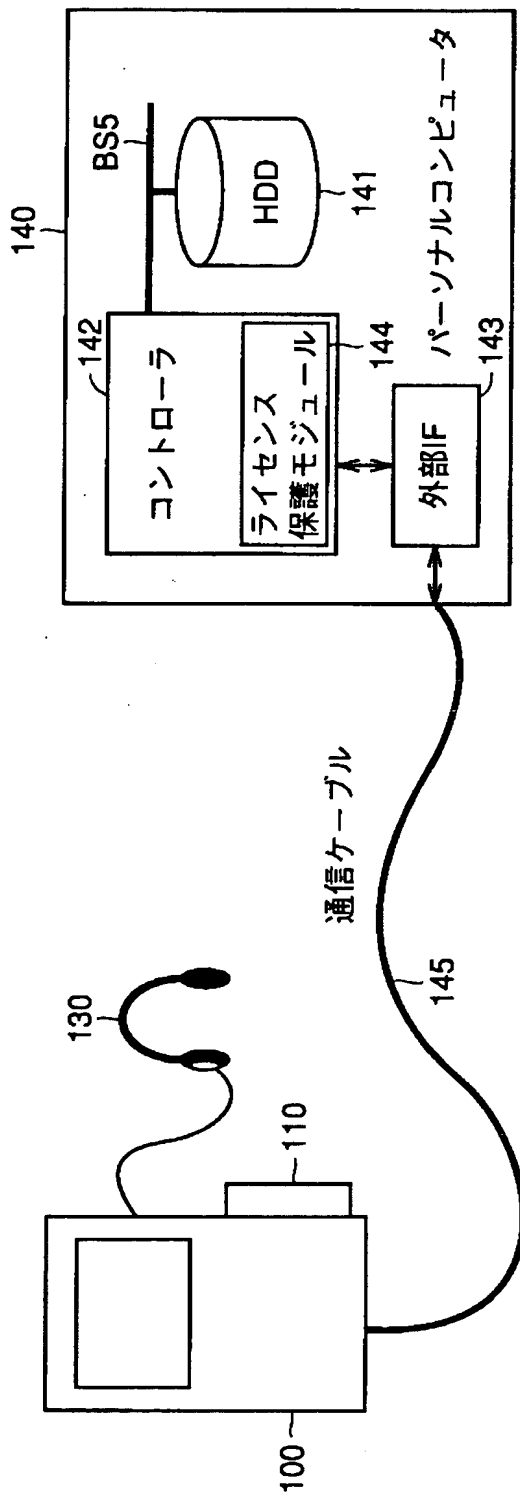


【図 16】

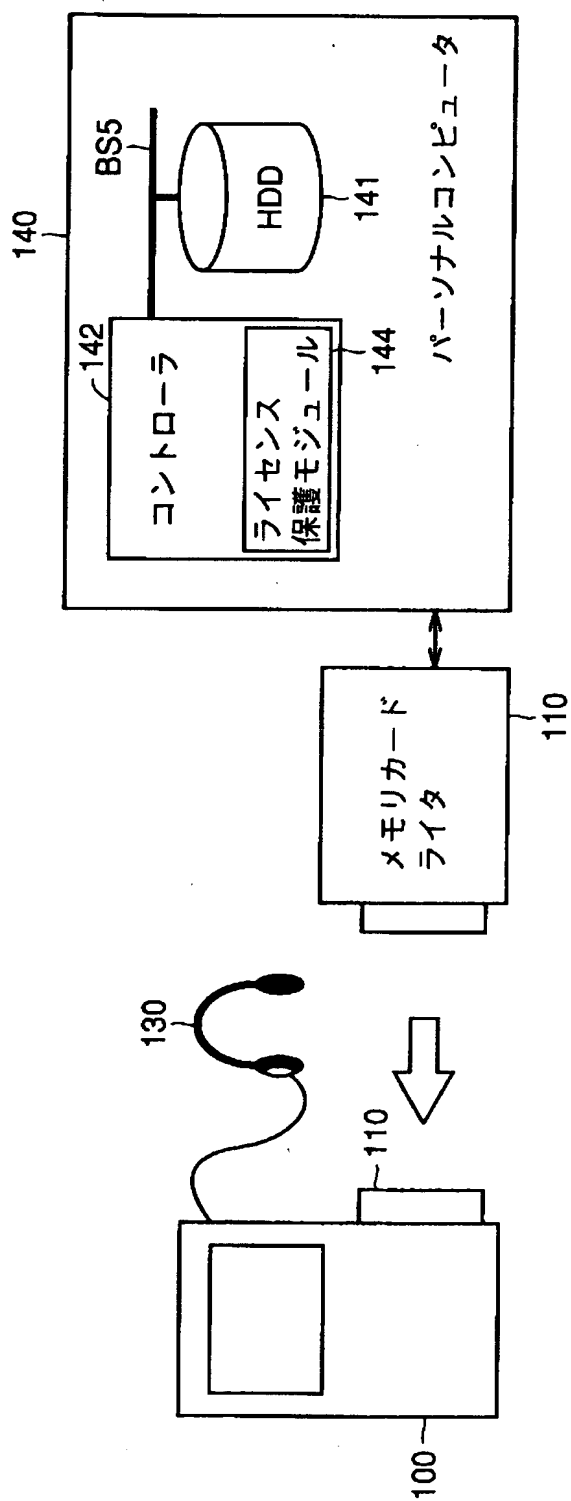
120



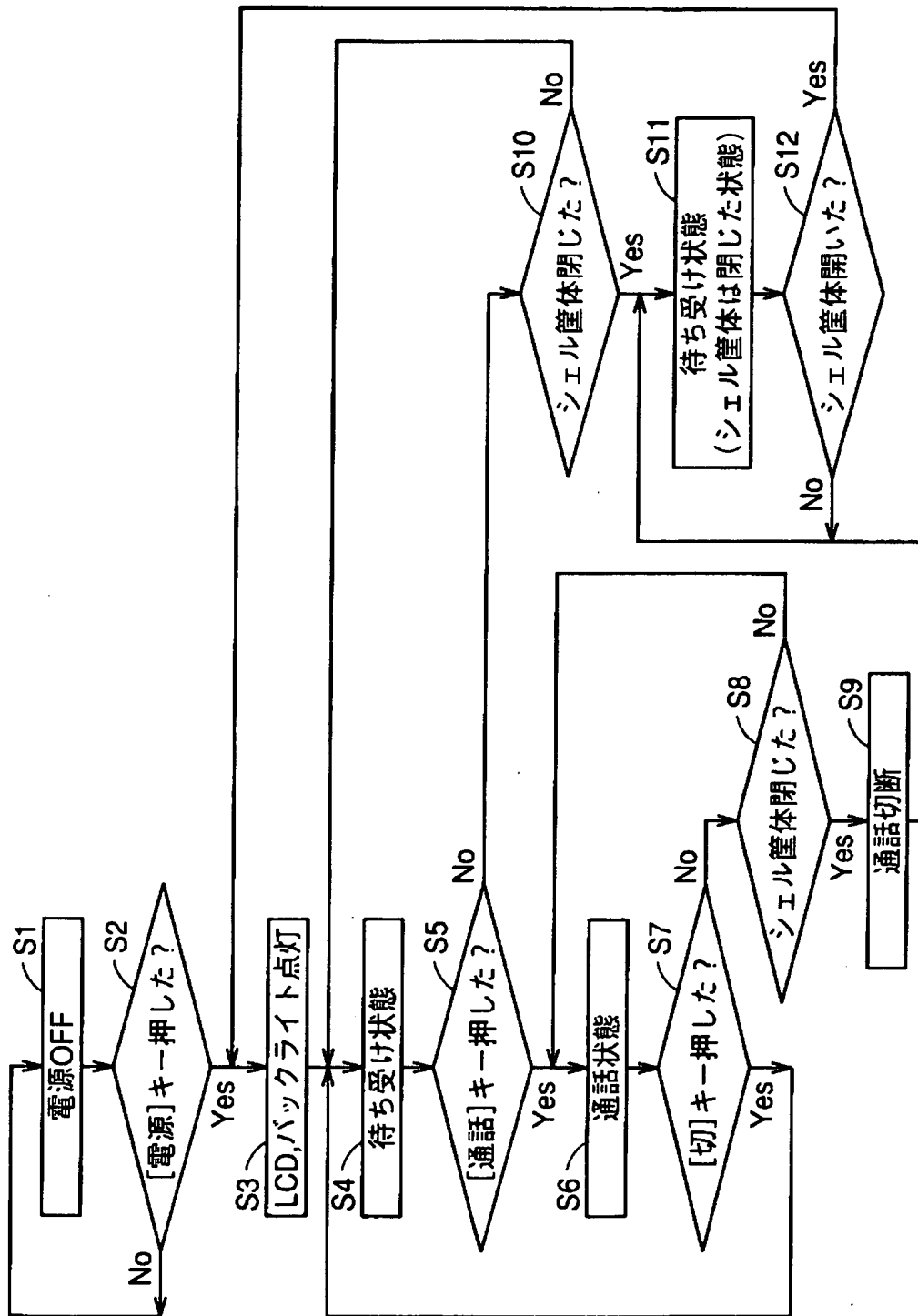
【図 17】



【図18】



【图 19】



【書類名】 要約書

【要約】

【課題】 筐体を閉じた後であってもダウンロードまたは再生することができるシェル型データ端末装置を提供する。

【解決手段】 シェル型携帯電話機100は、配信サーバから暗号化コンテンツデータをダウンロードし、再生する機能を有する。シェル型携帯電話機100は、シェル開閉検出部1117において、シェル型筐体の開閉状態を検出する。暗号化コンテンツデータをダウンロード中または再生中にシェル型筐体が閉じるとコントローラ1106は、ダウンロードまたは再生処理が完了するまでに必要な電源を供給するように電源供給部1116を制御する。これにより、シェル型筐体が閉じていても、ダウンロードまたは再生処理が完了する。

【選択図】 図7

出 願 人 履 歴 情 報

識別番号 [000001889]

1. 変更年月日 1993年10月20日
[変更理由] 住所変更
住 所 大阪府守口市京阪本通2丁目5番5号
氏 名 三洋電機株式会社